Probabilistic Hash-and-Sign with Retry in the Quantum Random Oracle Model[⋆]

Haruhisa Kosuge[1] and Keita Xagawa[2][0000−0002−6832−9940][⋆⋆]

[1] Japan Ministry of Defense, Japan
harucrypto@gmail.com
[2] Technology Innovation Institute, UAE
keita.xagawa@tii.ae

Abstract. A hash-and-sign signature based on a preimage-sampleable function (Gentry et al., STOC 2008) is secure in the quantum random oracle model if the preimage-sampleable function is collision-resistant (Boneh et al., ASIACRYPT 2011) or one-way (Zhandry, CRYPTO 2012). However, trapdoor functions in code-based and multivariate-quadratic-based signatures are not preimage-sampleable functions; for example, underlying trapdoor functions of the Courtois-Finiasz-Sendrier, Unbalanced Oil and Vinegar (UOV), and Hidden Field Equations (HFE) signatures are not surjections. Thus, such signature schemes adopt *probabilistic hash-and-sign with retry*. While Sakumoto et al. in PQCRYPTO 2011 showed the security of this paradigm in the classical random oracle model, their proof contains an error. Also, there is currently no known security proof for the probabilistic hash-and-sign with retry in the quantum random oracle model. We correct the proof in the random oracle model and give the first security proof in the quantum random oracle model for the probabilistic hash-and-sign with retry, assuming that the underlying trapdoor function is non-invertible, that is, it is hard to find a preimage of a given random value in the range. Our reduction from the non-invertibility assumption is tighter than the existing ones that apply only to signature schemes based on preimage-sampleable functions. We apply the security proof to code-based and multivariate-quadratic-based signatures. Additionally, we extend the proof into the multi-key setting and propose a generic method that provides security reduction without any security loss in the number of keys.

keywords: Post-quantum cryptography, digital signature, hash-and-sign, quantum random oracle model, preimage sampleable function.

1 Introduction

Hash-and-Sign Signature in the Random Oracle Model (ROM): A digital signature is an essential and versatile primitive since it supports non-repudiation and authentication; if a document is signed, the signer indeed signed it and cannot

[⋆] The full version is available at https://eprint.iacr.org/2022/1359.

[⋆⋆] Part of the work done while at NTT Corporation.

repudiate the signature. The standard security notion of the digital signature is existential unforgeability against chosen-message attack (EUF-CMA) [31]. Roughly speaking, a signature scheme is said to be EUF-CMA-secure if no efficient adversary can forge a signature even if the adversary can access a signing oracle, which captures non-repudiation and authentication. Hash-and-sign [5, 6] is a widely adopted paradigm for constructing practical signatures, along with Fiat-Shamir [28], in the ROM [5]. This paper focuses on hash-and-sign.

A hash-and-sign signature scheme is realized by a hard-to-invert function $\mathsf{F}\colon \mathcal{X} \to \mathcal{Y}$, its trapdoor $\mathsf{I}\colon \mathcal{Y} \to \mathcal{X}$, and a hash function $\mathsf{H}\colon \{0,1\}^* \to \mathcal{Y}$ modeled as a random oracle. To sign on a message m, a signer first computes $y = \mathsf{H}(r, m)$, where r is a random string, computes $x = \mathsf{I}(y)$, and outputs $\sigma = (r, x)$ as a signature. A verifier verifies the signature σ with the verification key F by checking if $\mathsf{H}(r, m) = \mathsf{F}(x)$ or not. We refer to this construction as *probabilistic hash-and-sign*; if r is an empty string, then *deterministic hash-and-sign*. The security properties of the trapdoor function are outlined as follows.

Non-invertibility (INV): It is hard to find a preimage of a challenge y that is uniformly chosen [34].

One-wayness (OW): It is hard to find a preimage of a challenge $y = \mathsf{F}(x)$ for x chosen from some distribution on $\mathcal{X}$ [5].

Collision-resistance (CR): It is hard to find a collision pair of F.

A prime example is a deterministic hash-and-sign using a trapdoor permutation such as RSA, which is EUF-CMA-secure in the ROM, assuming the OW of the trapdoor permutation [5]. Gentry, Peikert, and Vaikuntanathan proposed deterministic/probabilistic hash-and-sign based on a preimage-sampleable function (PSF) [30], which is a trapdoor function with additional conditions, e.g., surjection. Gentry et al. showed a tight reduction from the CR assumption of PSF to the *strong* EUF-CMA (sEUF-CMA) security of the deterministic/probabilistic hash-and-sign, and they constructed a collision-resistant PSF from lattices. Unfortunately, it is hard to build PSFs in code-based and multivariate-quadratic-based (MQ-based) cryptography; for example, F is not a surjection. In this case, the trapdoor I fails to invert y whose preimage does not exist. For such trapdoor functions, we employ the probabilistic hash-and-sign *with retry*, where a signer takes randomness r until r allows inversion of $y = \mathsf{H}(r, m)$. The Courtois-Finiasz-Sendrier (CFS) signature [19] in code-based cryptography and the Unbalanced Oil and Vinegar (UOV) [39] and Hidden Field Equations (HFE) signatures [49] in MQ-based cryptography use this paradigm. Sakumoto et al. [53] gave a security proof of the probabilistic hash-and-sign with retry in the ROM. However, their proof has a flaw in the simulation of the random oracle, which is pointed out by Chatterjee et al. [18].

Hash-and-Sign Signature in Quantum Random Oracle Model (QROM): Large-scale quantum computers will be able to break widely deployed public-key cryptography such as RSA and ECDSA because of Shor's algorithm [56]. Consequently, there has been a growing interest in post-quantum cryptography

Table 1: Summary of the security proofs for hash-and-sign in the QROM. DHaS, PHaS, and PHaSwR denote deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry. ϵ denotes the adversary's advantage in the game of the underlying assumption. q denotes the number of queries to the signing and random oracles.

Name	DHaS	PHaS	PHaSwR	Assumption	Security Bound
[14]	✓	✓	–	CR	$O(\epsilon_{\mathsf{cr}})$
[61]	✓	✓	–	OW/INV	$O(q^2\sqrt{\epsilon_{\mathsf{ow/inv}}})$
ext. of [59]	✓	✓	–	OW/INV	$O(q^4\epsilon_{\mathsf{ow/inv}})$
[17]	–	✓	–	EUF-NMA	$O(\epsilon_{\mathsf{nma}})$
Ours	-	✓	✓	INV	$O(q^2\epsilon_{\mathsf{inv}})$

(PQC). Recently NIST selected PQC candidates of public-key encryption/key-encapsulation mechanism (KEM) and digital signature for standardization [48]. Furthermore, NIST initiated an additional call for PQC digital signatures [47]. In the context of PQC, it is essential for signature schemes to provide EUF-CMA security in the QROM [14] since it models real-world quantum adversaries having *offline* access to the hash function. Unfortunately, schemes that are secure in the ROM are not always secure in the QROM, as demonstrated by separation results, including a signature scheme, by Yamakawa and Zhandry [60].

Table 1 summarizes studies on the EUF-CMA security of hash-and-sign signatures in the QROM. Boneh et al. [14] showed a tight reduction from the CR assumption of PSF using the history-free reduction. Zhandry [61] gave a reduction from the OW/INV assumptions[3], using a technique called semi-constant distribution[4]. Unfortunately, the semi-constant distribution technique incurs a square-root loss in the success probability. Yamakawa and Zhandry [59] gave the lifting theorem that shows that any search-type game is hard in the QROM if the game is hard in the ROM. They used the lifting theorem to show that an EUF-NMA-secure signature in the ROM is EUF-NMA-secure in the QROM, where NMA stands for No-Message Attack. By extending the results of [59], we obtain a reduction from the OW/INV assumptions of PSF. Chailloux and Debris-Alazard [17] gave a security proof of the probabilistic hash-and-sign based on non-PSF trapdoor functions. Also, Grilo, Hövelmanns, Hülsing, and Majenz [32] gave a reduction from the EUF-RMA security of a signature scheme for fixed-length messages, where RMA stands for Random-Message Attack[5]. However, there is no known reduction to the EUF-RMA security of the underlying signature from the OW/INV assumptions of trapdoor functions. Regarding the

[3] For PSF, tight reductions exist both from OW to INV and from INV to OW.

[4] Zhandry [61] proved the EUF-CMA security by assuming that the trapdoor permutation is one-way. The security proof applies to a case where the PSF is either one-way or non-invertible.

[5] A signer chooses r, computes $m' = \mathsf{H}(r, m)$, and signs on m' by using a signing algorithm of the signature scheme for fixed-length messages, and outputs (r, σ).

probabilistic hash-and-sign with retry, there is no valid proof even in the ROM. Naturally, there is no proof in the QROM, which has an impact on the security evaluation of code-based and MQ-based signatures. Our central question is:

Q1. Is there an EUF-CMA *security proof for the probabilistic hash-and-sign with retry? How tight is the security proof?*

Provable Security in Multi-key Setting: The EUF-CMA security is sometimes insufficient to ensure the security of the digital signature in the real world since exploiting one of many users may be sufficient for a real-world adversary to intrude into a system. We must consider the EUF-CMA security *in the multi-key setting*, the M-EUF-CMA security in short. The adversary, given multiple verification keys, tries to forge a valid signature for one of the verification keys. If the adversary can gain an advantage by targeting multiple keys (*multi-key attack*), the M-EUF-CMA security degrades with the number of keys (or users). NIST mentioned resistance to multi-key attacks as a "desirable property" in their call for proposals [46] of the PQC standardization project. We can ensure resistance against multi-key attacks if there is no security loss in the number of keys. Thus, our additional question is:

Q2. Is there an M-EUF-CMA *security proof for hash-and-sign without any security loss in the number of keys?*

The technique of including an entire verification key as part of the input for the hash function is known as *key prefixing*, which enables one to separate the domain of the hash function for each verification key. Schnorr signature adopts key prefixing to show a tight reduction in the multi-key setting [44]. Similarly, Duman et al. [25] proposed a technique called *prefix hashing* for the Fujisaki-Okamoto transform of KEM. Prefix hashing is a technique in which the hash function includes only a small unpredictable portion of a verification key, resulting in a smaller increase in execution time compared to the key prefixing.

1.1 Contributions

Security Proof of Probabilistic Hash-and-Sign with Retry in the QROM: We affirmatively answer Q1. We correct the existing proof of [53] in the ROM and establish a security proof in the QROM (*main theorem*) based on the corrected ROM proof. Additionally, the main theorem applies to the probabilistic hash-and-sign *without retry*. Furthermore, we show that a signature scheme is sEUF-CMA-secure if the underlying trapdoor function is an injection. Our reduction is tighter than the existing ones that apply to the probabilistic hash-and-sign without retry only [61, 17, 59]. Fig. 1 shows a diagram of the reduction. The main theorem comprises two reductions; EUF-NMA ⇒ EUF-CMA and INV ⇒ EUF-NMA, where X ⇒ Y inidicates a reduction from X to Y. The main theorem has a security bound $(2q_{\mathsf{qro}} + 1)^2 \epsilon_{\mathsf{inv}}$, where q_{qro} is a bound on the number of random oracle queries and ϵ_{inv} is an advantage of breaking the INV.

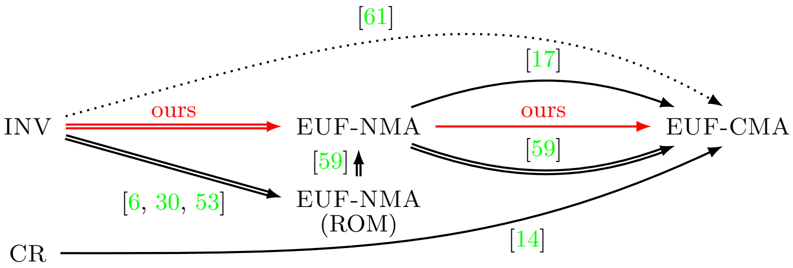

Fig. 1: A diagram illustrating reductions of hash-and-sign in the QROM. Red arrows represent our results, while solid, double, and dotted arrows represent tight reductions, reductions with linear or quadratic loss, and non-tight reductions.

Proof Idea: We provide a technical overview of the main theorem. To prove EUF-NMA ⇒ EUF-CMA, we assume that the following two values are statistically or computationally indistinguishable:

- x obtained after retrying y until y becomes invertible by the trapdoor I.
- x obtained by a simulator that does not use the trapdoor I.

The proof by Sakumoto et al. [53] simulates the signing oracle by programming H such that $\mathsf{H}(r, m)$ outputs $\mathsf{F}(x)$ for (r, x) chosen without using I. Since we do not assume that $\mathsf{F}(x)$ is uniform, the output of H may become biased. Therefore, their proof is flawed, and the following two additional steps are required.

First, we *adapively* reprogram the random function. Given a message m, the signing oracle repeatedly reprograms H such that $\mathsf{H}(r, m) = y$ holds for randomly chosen $(r, y) \in \mathcal{R} \times \mathcal{Y}$, and this reprogramming continues until the trapdoor I can provide a preimage $x \in \mathcal{X}$ of y ($\mathsf{F}(x) = y$). In the ROM, this reprogramming is feasible as long as r chosen in the signing oracle has not been queried in advance. In the QROM, we employ the tight adaptive reprogramming technique [32].

Next, we cancel the reprogramming during retries, specifically, reprogramming for (r, y) such that $\mathsf{I}(y)$ fails to invert, to make the simulation feasible based on the aforementioned assumption. We utilize the fact that r is chosen independently of the queried m in the signing oracle, which allows us to choose r used for reprogramming during retries at the beginning of the game. We define a set of such prechosen r as $\mathcal{S}$. Then, we *puncture* H on $\mathcal{S}$ [1], that is, a modification of H such that the adversary cannot make a query for H on $\mathcal{S}$. In the ROM, this punctuation is feasible as long as the adversary does not make queries for H on $\mathcal{S}$. In the QROM, we utilize the semi-classical One-way to Hiding lemma [1]. As a result, we can cancel the reprogramming, as the adversary cannot distinguish whether H is reprogrammed during retries or not. After the cancelation, the EUF-NMA adversary can simulate the signing oracle.

Regarding INV ⇒ EUF-NMA, the INV adversary gives his challenge y to the EUF-NMA adversary and outputs x^* that is included in the final output

(m^*, r^*, x^*) of the EUF-NMA adversary. In the ROM, the INV adversary randomly selects one query to H and returns his challenge y as in [53]. In the QROM, we use the measure-and-reprogram technique developed by Don et al. [23], incurring a security loss of $(2q_{\mathsf{qro}} + 1)^2$. As far as we know, this usage is new in the context of the probabilistic hash-and-sign.

Applications: Applying the main theorem, we enhance the EUF-CMA security of Wave [2] and give the first proof for the sEUF-CMA security of the modified CFS signature [20] as well as the EUF-CMA security of Rainbow [22], GeMSS [16], MAYO [10], QR-UOV [29], and PROV [26] in the QROM. To the best of our knowledge, the main theorem encompasses all existing hash-and-sign signatures such that reductions of INV ⇒ (s)EUF-CMA are known in the ROM. NIST has recently announced additional candidates for post-quantum signatures. NIST has the intention of standardizing schemes that are not based on structured lattices [47]. The main theorem has wide application in code-based and MQ-based cryptography, promising candidates for this call. The additional candidates include Wave, MAYO, QR-UOV, and PROV. Notably, QR-UOV and PROV have utilized the main theorem in their specifications [29, 26].

Security Proof in Multi-Key Setting: We introduce a generic method for establishing a reduction from the property of trapdoor functions in the single-instance setting to the security of the hash-and-sign with prefix hashing in the multi-key setting. The core idea behind this generic method is to apply pairs of randomly generated transformations $\{\mathsf{L}_j, \mathsf{R}_j\}_j$ to a single verification key F'. Here, F' belongs to another trapdoor function, assumed to be non-invertible. This process effectively simulates multiple verification keys through $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_j$. Assuming the indistinguishability between $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_j$ and real verification keys $\{\mathsf{F}_j\}_j$, we show a reduction of INV ⇒ M-EUF-CMA with a security bound $(2q_{\mathsf{qro}} + 1)^2 \epsilon_{\mathsf{inv}}$ and a tight reduction of CR ⇒ M-sEUF-CMA. Since there is no security loss in the number of keys, we can affirmatively answer Q2. Furthermore, we apply the generic method to some hash-and-sign signatures. In these applications, we introduce some computational problems that can computationally ensure the indistinguishability between $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_j$ and $\{\mathsf{F}_j\}_j$. However, establishing the hardness of these computational problems remains an open problem as they have not been extensively studied.

Concurrent Work: Liu, Jiang, and Zhao [41] show the EUF-CMA security of the deterministic/probabilistic hash-and-sign based on trapdoor permutations in the QROM by using the measure-and-reprogram technique by Don et al. [23]. Their security bound is $(2(q_{\mathsf{qro}} + q_{\mathsf{sign}} + 1) + 1)^2 \epsilon_{\mathsf{inv}}$, where q_{sign} is a bound on the number of signing queries. They also give an analysis for (H)IBE in the QROM. Our work has two advantages over their work on hash-and-sign. First, our work has wider applications since it has generality in its application to probabilistic hash-and-sign with/without retry, in contrast to the restriction of [41] to the deterministic/probabilistic hash-and-sign[6] and allows the usage of non-PSF trapdoor functions, generalization of trapdoor permutations. Second, the main theorem has the bound $(2q_{\mathsf{qro}}+1)^2\epsilon_{\mathsf{inv}}$, which does not include q_{sign}.

Two papers [21, 3] recently pointed out a subtle flaw in the security proofs of Fiat-Shamir with aborts [42] in the QROM [37, 32]. The flaw stems from the bias introduced by the simulation with abort, which we treat in EUF-NMA ⇒ EUF-CMA carefully. We note that the games in the corrected proof in [3] are defined in the same spirit as our proof of EUF-NMA ⇒ EUF-CMA while the proof techniques and the details are different. Leveraging its structural resemblance to the probabilistic hash-and-sign with retry, we present an alternative security proof for the Fiat-Shamir with aborts by employing the same techniques used in the main theorem of this paper.

Organization: Section 2 gives notations, definitions, and so on. Section 3 reviews the existing security proofs in the (Q)ROM. Section 4 presents the main theorem and discusses applications. In Section 5, we describe the generic method applied in the multi-key setting. Appendix A demonstrates a flaw in the security proof of concurrent work [41]. Appendix B presents security proofs of hash-and-sign signatures reviewed in Appendix C. Appendices D and E show missing proofs for the theorem in the multi-key setting. Appendix F shows applications of the generic method in the multi-key setting. Appendix G provides a security proof for the Fiat-Shamir with aborts, employing the same techniques as the main theorem.

2 Preliminaries

2.1 Notations and Terminology

For $n \in \mathbb{N}$, we let $[n] \coloneqq \{1,\dots,n\}$. We write any symbol for sets in calligraphic font. For a finite set $\mathcal{X}$, $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$ and $\mathsf{U}(\mathcal{X})$ is the uniform distribution over $\mathcal{X}$. By $x \leftarrow_\$ \mathcal{X}$ and $x \leftarrow \mathcal{D}_\mathcal{X}$, we denote the sampling of an element from $\mathsf{U}(\mathcal{X})$ and $\mathcal{D}_\mathcal{X}$ (distribution on $\mathcal{X}$). We denote a set of functions having a domain $\mathcal{X}$ and a range $\mathcal{Y}$ by $\mathcal{Y}^\mathcal{X}$.

We write any symbol for functions in sans-serif font and adversaries in calligraphic font. Let F be a function, and $\mathcal{A}$ be an adversary. We denote by $y \leftarrow \mathsf{F}^{\mathsf{H}}(x)$ and $y \leftarrow \mathcal{A}^{\mathsf{H}}(x)$ (resp., $y \leftarrow \mathsf{F}^{|\mathsf{H}\rangle}(x)$ and $y \leftarrow \mathcal{A}^{|\mathsf{H}\rangle}(x)$) probabilistic computations of F and $\mathcal{A}$ on input x with a classical (resp., quantum) oracle access to a function H. If F and $\mathcal{A}$ are deterministic, we write $y \coloneqq \mathsf{F}^{\mathsf{H}}(x)$ and $y \coloneqq \mathcal{A}^{\mathsf{H}}(x)$. For a random function H, we denote by $\mathsf{H}^{x^*\mapsto y^*}$ a function such that $\mathsf{H}^{x^*\mapsto y^*}(x) = \mathsf{H}(x)$ for $x \neq x^*$ and $\mathsf{H}^{x^*\mapsto y^*}(x^*) = y^*$. The notation $\mathsf{G}^{\mathcal{A}} \Rightarrow y$ denotes an event in which a game G played by $\mathcal{A}$ returns y.

We denote 1 if the Boolean statement is true $\top$ and 0 if the statement is false $\bot$. A binary operation $a \overset{?}{=} b$ outputs $\top$ if $a = b$ and outputs $\bot$ otherwise.

[6] Although the deterministic hash-and-sign is not in our scope, it can be transformed into the probabilistic one with a small tweak.

```
GAME: EUF-CMA
1 $\mathcal{Q} := \emptyset$
2 $(vk, sk) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
3 $(m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}}(vk)$
4 if $m^* \in \mathcal{Q}$ then
5     return 0
6 return $\mathsf{Sig.Verify}(vk, m^*, \sigma^*)$
```

```
$\mathsf{Sign}(m_i)$
1 $\sigma_i \leftarrow \mathsf{Sig.Sign}(sk, m_i)$
2 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
3 return $\sigma_i$
```

```
GAME: EUF-NMA
1 $(vk, sk) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
2 $(m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{nma}}(vk)$
3 return $\mathsf{Sig.Verify}(vk, m^*, \sigma^*)$
```

Fig. 2: EUF-CMA and EUF-NMA games

2.2 Digital Signature and Trapdoor Function

Definition 1 (Digital Signature). *A digital signature scheme* Sig *consists of three algorithms:*

$\mathsf{Sig.KeyGen}(1^\lambda)$*: This algorithm takes the security parameter* 1^λ *as input and outputs a verification key* vk *and a signing key* sk*.*

$\mathsf{Sig.Sign}(sk, m)$*: This algorithm takes a signing key* sk *and a message* m *as input and outputs a signature* σ*.*

$\mathsf{Sig.Vrfy}(vk, m, \sigma)$*: This algorithm takes a verification key* vk*, a message* m*, and a signature* σ *as input, and outputs* $\top$ *(acceptance) or* $\bot$ *(rejection).*

We say Sig *is correct if, for all* $(vk, sk) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$ *and for all* $m \in \mathcal{M}$, $\Pr[\mathsf{Sig.Vrfy}(vk, m, \mathsf{Sig.Sign}(sk, m)) = \bot]$ *is negligible.*

Definition 2 (Security of Signature). *Let* Sig *be a signature scheme. Using games given in Fig. 2, we define advantage functions of adversaries playing* EUF-CMA *(Existential UnForgeability against Chosen-Message Attack) and* EUF-NMA *(No-Message Attack) games against* Sig *as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\left[\mathsf{EUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{EUF-NMA}}(\mathcal{A}_{\mathsf{nma}}) = \Pr\left[\mathsf{EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma}}} \Rightarrow 1\right]$*, respectively. Also, we define an advantage function for an* sEUF-CMA *(strong* EUF-CMA*) game as* $\mathrm{Adv}_{\mathsf{Sig}}^{\text{sEUF-CMA}}(\mathcal{A}_{\mathsf{cma}}) = \Pr\left[\mathsf{sEUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$*, where the* sEUF-CMA *game is identical to the* EUF-CMA *game except that Line 4 of the game is changed as "* **if** $(m^*, \sigma^*) \in \mathcal{Q}$ **then***" and Line 2 of the signing oracle is changed as "*$\mathcal{Q} := \mathcal{Q} \cup \{(m_i, \sigma_i)\}$*". We say* Sig *is* EUF-CMA*-secure,* sEUF-CMA*-secure, or* EUF-NMA*-secure if its corresponding advantage is negligible for any efficient adversary in the security parameter.*

Definition 3 (Trapdoor Function). *A trapdoor function* T *consists of three algorithms:*

$\mathsf{Gen}(1^\lambda)$*: This algorithm takes the security parameter* 1^λ *as input and outputs a function* F *with a trapdoor* I *of* F*.*

$\mathsf{F}(x)$*: This algorithm takes* $x \in \mathcal{X}$ *and deterministically outputs* $\mathsf{F}(x) \in \mathcal{Y}$*.*

$\mathsf{I}(y)$*: This algorithm takes* $y \in \mathcal{Y}$ *and outputs* $x \in \mathcal{X}$*, s.t.,* $\mathsf{F}(x) = y$*, or outputs* $\bot$*.*

```
GAME: INV
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$y \leftarrow_\$ \mathcal{Y}$
$x^* \leftarrow \mathcal{B}_{\mathsf{inv}}(\mathsf{F}, y)$
return $\mathsf{F}(x^*) \overset{?}{=} y$
```

```
GAME: OW
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$x \leftarrow \mathcal{D}_\mathcal{X}$
$y := \mathsf{F}(x)$
$x^* \leftarrow \mathcal{B}_{\mathsf{ow}}(\mathsf{F}, y)$
return $\mathsf{F}(x^*) \overset{?}{=} y$
```

```
GAME: CR
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(x_1^*, x_2^*) \leftarrow \mathcal{B}_{\mathsf{cr}}(\mathsf{F})$
return $\mathsf{F}(x_1^*) \overset{?}{=} \mathsf{F}(x_2^*)$
```

Fig. 3: INV (non-INVertibility), OW (One-Wayness), and CR (Collision-Resistance) games

Definition 4 (Security of Trapdoor Function). *Let T be a trapdoor function. Using games given in Fig. 3, we define advantage functions of adversaries playing the* INV *(non-INVertibility)* [7]*,* OW *(One-Wayness), and* CR *(Collision-Resistance) games against T as* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{INV}}(\mathcal{B}_{\mathsf{inv}}) = \Pr\left[\mathsf{INV}^{\mathcal{B}_{\mathsf{inv}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{OW}}(\mathcal{B}_{\mathsf{ow}}) = \Pr\left[\mathsf{OW}^{\mathcal{B}_{\mathsf{ow}}} \Rightarrow 1\right]$*, and* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{CR}}(\mathcal{B}_{\mathsf{cr}}) = \Pr\left[\mathsf{CR}^{\mathcal{B}_{\mathsf{cr}}} \Rightarrow 1\right]$*, respectively. We say T is non-invertible, one-way, or collision-resistant if its corresponding advantage is negligible in the security parameter for any efficient adversary.*

2.3 Preimage-Sampleable Function

In the ROM, hash-and-sign is EUF-CMA-secure when instantiated with a preimage-sampleable function (PSF) [30]. We first define its weakened version.

Definition 5 (Weak Preimage-Sampleable Function (WPSF)). *A WPSF T is a trapdoor function that is equipped with an additional function $\mathsf{SampDom}(\mathsf{F})$, which takes as input $\mathsf{F} \in \mathcal{Y}^\mathcal{X}$ and outputs some $x \in \mathcal{X}$.*

We then review PSF:

Definition 6 (Preimage-Sampleable Function (PSF) [30]). *A WPSF T is said to be a PSF if it satisfies three conditions for any $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$:*

Condition 1*: $\mathsf{F}(x)$ is uniform over $\mathcal{Y}$ for $x \leftarrow \mathsf{SampDom}(\mathsf{F})$.*
Condition 2*: $x \leftarrow \mathsf{I}(y)$ follows a distribution of $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ given $\mathsf{F}(x) = y$.*
Condition 3*: $\mathsf{I}(y)$ outputs x satisfying $\mathsf{F}(x) = y$ for any $y \in \mathcal{Y}$.*

If T is collision-resistant PSF, it satisfies the above conditions plus the following:

Condition 4*: For any $y \in \mathcal{Y}$, the conditional min-entropy of $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ given $\mathsf{F}(x) = y$ is at least $\omega(\log(\lambda))$.*

In the proof of EUF-CMA security, a trapdoor function may not be a PSF, but it must be a WPSF that satisfies a relaxed version of **Condition 2** that ensures indistinguishability between $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ and $x \leftarrow \mathsf{I}(y)$. To define this relaxed condition, we introduce a game shown in Fig. 4.

[7] In general, *non-invertibility* of trapdoor functions is called *one-wayness* [30, 53, 17]. We make a distinction between them depending on the way to choose challenges (INV follows [34] and OW follows [5]).

```
GAME: $\mathsf{PS}_b$
1 $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
2 $b^* \leftarrow \mathcal{D}_{\mathsf{ps}}^{\mathsf{Sample}_b}(\mathsf{F})$
3 return $b^*$

$\mathsf{Sample}_0()$
1 repeat
2     $y_i \leftarrow_\$ \mathcal{Y}$
3     $x_i \leftarrow \mathsf{I}(y_i)$
4 until $x_i \neq \bot$
5 return $x_i$

$\mathsf{Sample}_1()$
1 $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
2 return $x_i$
```

Fig. 4: PS (Preimage Sampling) game

```
GAME: M-EUF-CMA
1 $\mathcal{Q} := \emptyset$
2 for $j \in [q_{\mathsf{key}}]$ do
3     $(vk_j, sk_j) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
4 $(j^*, m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{cma^m}}^{\mathsf{Sign}}(\{vk_j\}_{j \in [q_{\mathsf{key}}]})$
5 if $(j^*, m^*) \in \mathcal{Q}$ then
6     return 0
7 return $\mathsf{Sig.Verify}(vk_{j^*}, m^*, \sigma^*)$

$\mathsf{Sign}(j, m_i)$
1 $\sigma_i \leftarrow \mathsf{Sig.Sign}(sk_j, m_i)$
2 $\mathcal{Q} := \mathcal{Q} \cup \{(j, m_i)\}$
3 return $\sigma_i$
```

Fig. 5: M-EUF-CMA (Multi-key EUF-CMA) game

Definition 7 (Preimage Sampling (PS) Game). *Let* T *be a WPSF. Using a game defined in Fig. 4, we define an advantage function of an adversary playing the* PS *game against* T *as* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{PS}}(\mathcal{D}_{\mathsf{ps}}) = \left|\Pr\left[\mathsf{PS}_0^{\mathcal{D}_{\mathsf{ps}}} \Rightarrow 1\right] - \Pr\left[\mathsf{PS}_1^{\mathcal{D}_{\mathsf{ps}}} \Rightarrow 1\right]\right|$. *We say* T *is preimage-simulatable if its advantage is negligible for any efficient adversary.*

2.4 Security Games in Multi-key/Multi-instance Settings

Definition 8 (Security of Signature in Multi-key Setting [38]). *Let* Sig *be a signature scheme. Using a game given in Fig. 5, we define advantage functions of adversaries playing the* M-EUF-CMA *and* M-sEUF-CMA *(Multi-key* EUF-CMA/sEUF-CMA*) games against* Sig *as* $\mathrm{Adv}_{\mathsf{Sig}}^{\mathrm{M\text{-}EUF\text{-}CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\mathsf{M\text{-}EUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$ *and* $\mathrm{Adv}_{\mathsf{Sig}}^{\mathrm{M\text{-}sEUF\text{-}CMA}}(\mathcal{A}_{\mathsf{cma^m}}) = \Pr\left[\mathsf{M\text{-}sEUF\text{-}CMA}^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]$, *where the* M-sEUF-CMA *game is identical to the* M-EUF-CMA *game except that Line 5 of the game is changed as "* **if** $(j^*, m^*, \sigma^*) \in \mathcal{Q}$ **then***" and Line 2 of the signing oracle is changed as "*$\mathcal{Q} := \mathcal{Q} \cup \{(j, m_i, \sigma_i)\}$*". We say* Sig *is* M-EUF-CMA*-secure or* M-sEUF-CMA*-secure if its corresponding advantage is negligible for any efficient adversary in the security parameter.*

Definition 9 (INV, CR, and PS in Multi-instance Setting). *Let* T *be a trapdoor function or WPSF. Using games given in Fig. 6, we define advantage functions of adversaries playing the* M-INV*,* M-CR*, and* M-PS *(Multi-instance non-invertibility, collision resistance, and preimage sampling) games against* T *as* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{M\text{-}INV}}(\mathcal{B}_{\mathsf{inv^m}}) = \Pr\left[\mathsf{M\text{-}INV}^{\mathcal{B}_{\mathsf{inv^m}}} \Rightarrow 1\right]$, $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{M\text{-}CR}}(\mathcal{B}_{\mathsf{cr^m}}) = \Pr\left[\mathsf{M\text{-}CR}^{\mathcal{B}_{\mathsf{cr^m}}} \Rightarrow 1\right]$, *and* $\mathrm{Adv}_{\mathsf{T}}^{\mathrm{M\text{-}PS}}(\mathcal{D}_{\mathsf{ps^m}}) = \left|\Pr\left[\mathsf{M\text{-}PS}_0^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{M\text{-}PS}_1^{\mathcal{D}_{\mathsf{ps^m}}} \Rightarrow 1\right]\right|$, *respectively. We*

```
GAME: M-INV
for $j \in [q_{\mathsf{inst}}]$ do
    $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$
    $y_j \leftarrow_\$ \mathcal{Y}$
$(j^*, x^*) \leftarrow \mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}(\{(\mathsf{F}_j, y_j)\}_{j \in [q_{\mathsf{inst}}]})$
return $\mathsf{F}_{j^*}(x^*) \overset{?}{=} y_{j^*}$
```

```
GAME: M-CR
for $j \in [q_{\mathsf{inst}}]$ do
    $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$;
$(j^*, x_1^*, x_2^*) \leftarrow \mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}(\{\mathsf{F}_j\}_{j \in [q_{\mathsf{inst}}]})$
return $\mathsf{F}_{j^*}(x_1^*) \overset{?}{=} \mathsf{F}_{j^*}(x_2^*)$
```

```
GAME: M-PS_b
for $j \in [q_{\mathsf{inst}}]$ do
    $(\mathsf{F}_j, \mathsf{I}_j) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$
$b^* \leftarrow \mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}^{\mathsf{Sample}_b}(\{\mathsf{F}_j\}_{j \in [q_{\mathsf{inst}}]})$
return $b^*$
```

```
$\mathsf{Sample}_0(j)$
repeat
    $y_i \leftarrow_\$ \mathcal{Y}$
    $x_i \leftarrow \mathsf{I}_j(y_i)$
until $x_i \neq \bot$
return $x_i$
```

```
$\mathsf{Sample}_1(j)$
$x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$
return $x_i$
```

Fig. 6: M-INV, M-CR, and M-PS (Multi-instance INV, CR, and PS) games

```
$\mathsf{HaS}[\mathsf{T}, \mathsf{H}].\mathsf{KeyGen}(1^\lambda)$
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
return $(\mathsf{F}, \mathsf{I})$
```

```
$\mathsf{HaS}[\mathsf{T}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}, m)$
repeat
    $r \leftarrow_\$ \mathcal{R}$
    $x \leftarrow \mathsf{I}(\mathsf{H}(r, m))$
until $x \neq \bot$
return $(r, x)$
```

```
$\mathsf{HaS}[\mathsf{T}, \mathsf{H}].\mathsf{Vrfy}(\mathsf{F}, m, (r, x))$
return $\mathsf{F}(x) \overset{?}{=} \mathsf{H}(r, m)$
```

Fig. 7: Algorithms of the probabilistic hash-and-sign with retry

say T *is multi-instance non-invertible, multi-instance collision-resistant, or multi-instance preimage-simulatable if its corresponding advantage is negligible in the security parameter for any efficient adversary.*

2.5 Hash-and-Sign Paradigm

Fig. 7 shows algorithms of the probabilistic hash-and-sign with retry, and $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ is a signature scheme using a trapdoor function T and a hash function H. If $\mathsf{HaS}[\mathsf{T}, \mathsf{H}].\mathsf{Sign}$ outputs a signature without retry, $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ instantiates the probabilistic hash-and-sign. If r is empty, $\mathsf{HaS}[\mathsf{T}, \mathsf{H}]$ instantiates the deterministic hash-and-sign.

2.6 Quantum Random Oracle Model (QROM)

In the ROM, a hash function $\mathsf{H} : \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ is modeled as a random function $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$. The random function is under the control of the challenger, and the adversary makes queries to the random oracle (*random oracle queries*) to compute the hash values. In the ROM, the challenger can choose $y \leftarrow_\$ \mathcal{Y}$ and program $\mathsf{H} := \mathsf{H}^{(r,m) \mapsto y}$ for queried (r, m) on-the-fly instead of choosing $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$ at the beginning (lazy sampling technique).

In the QROM, the adversary makes queries to H in a superposition of many different values, e.g., $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle$. The challenger computes H and gives

```
GAME: $\mathsf{AR}_b$
$\mathsf{H}_0 \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
$\mathsf{H}_1 := \mathsf{H}_0$
$b^* \leftarrow \mathcal{D}_{\mathsf{ar}}^{|\mathsf{H}_b\rangle,\mathsf{Repro}}()$
return $b^*$

$\mathsf{Repro}(m_i)$
$r_i \leftarrow \mathcal{D}_{\mathcal{R}}$
$y_i \leftarrow_\$ \mathcal{Y}$
$\mathsf{H}_1 := \mathsf{H}_1^{(r_i,m_i)\mapsto y_i}$
return $r_i$
```

Fig. 8: AR (Adaptive Reprogramming) game

a superposition of the results to the adversary, $\sum_{(r,m)} \alpha_{r,m} |r,m\rangle |y \oplus \mathsf{H}(r,m)\rangle$. Due to the nature of superposition queries in the QROM, traditional proof techniques like lazy sampling used in the ROM cannot be directly applied in the QROM. However, some works enable one to adaptively reprogram H in the security game [58, 35, 23, 32]. Among the works, we use the tight adaptive reprogramming technique [32] and the measure-and-reprogram technique [23]. Also, we use the semi-classical O2H technique [1].

2.7 Proof Techniques in QROM

We introduce three techniques employed in proving the main theorem.

Tight Adaptive Reprogramming Technique [32]: Fig. 8 shows a game called AR (Adaptive Reprogramming) game, in which the adversary $\mathcal{D}_{\mathsf{ar}}$ attempts to distinguish H_0 (no reprogramming) from H_1 (reprogrammed by Repro). For i-th reprogramming query, the challenger reprograms H_1 for $r_i \leftarrow \mathcal{D}_{\mathcal{R}}$ and $y_i \leftarrow_\$ \mathcal{Y}$, and gives r_i to $\mathcal{D}_{\mathsf{ar}}$. Let ϵ be a bound on the maximum probability of $r \leftarrow \mathcal{D}_{\mathcal{R}}$, that is, $\max_{\hat{r}\in\mathcal{R}} \Pr[r = \hat{r} : r \leftarrow \mathcal{D}_{\mathcal{R}}] \le \epsilon$. A distinguishing advantage of the AR game is defined by $\mathrm{Adv}_{\mathsf{H}}^{\mathrm{AR}}(\mathcal{D}_{\mathsf{ar}}) = \left|\Pr\left[\mathsf{AR}_0^{\mathcal{D}_{\mathsf{ar}}} \Rightarrow 1\right] - \Pr\left[\mathsf{AR}_1^{\mathcal{D}_{\mathsf{ar}}} \Rightarrow 1\right]\right|$.

Lemma 1 (Tight Adaptive Reprogramming Technique [32, Proposition 2]). *For any quantum* AR *adversary $\mathcal{D}_{\mathsf{ar}}$ issuing at most q_{rep} classical reprogramming queries and q_{qro} (quantum) random oracle queries to H_b, the distinguishing advantage of the* AR *game is bounded by*

$$\mathrm{Adv}_{\mathsf{H}}^{\mathrm{AR}}(\mathcal{D}_{\mathsf{ar}}) \le \frac{3}{2} q_{\mathsf{rep}} \sqrt{q_{\mathsf{qro}}\epsilon}.$$

Especially, if $\mathcal{D}_{\mathcal{R}}$ is the uniform distribution $\mathsf{U}(\mathcal{R})$, then ϵ is equal to $\frac{1}{|\mathcal{R}|}$.

Measure-and-Reprogram Technique [23]: Let $\mathcal{A}$ be a quantum adversary playing a search-type game making q_{qro} quantum queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$. A two-stage algorithm S comprises S_1 and S_2, and it operates with black-box access to $\mathcal{A}$ as follows:

1. Choose $(i,b) \leftarrow_\$ ([q_{\mathsf{qro}}] \times \{0,1\}) \cup \{(q_{\mathsf{qro}}+1, 0)\}$.
2. Run $\mathcal{A}$ with H until i-th query.
3. Measure i-th query and output (r,m) as the output of S_1.

4. Given a random θ, reprogram $\mathsf{H}' = \mathsf{H}^{(r,m)\mapsto\theta}$.
5. If $i = q_{\mathsf{qro}} + 1$, then go to Step 8.
6. Answer i-th query with H (if $b = 0$) or H' (if $b = 1$).
7. Run $\mathcal{A}$ with H' until the end.
8. Output $\mathcal{A}$'s output z (possibly quantum) as the output of S_2.

Then, the following lemma holds for S and $\mathcal{A}$:

Lemma 2 (Measure-and-Reprogram Technique [23, Theorem 2]). *For any quantum adversary $\mathcal{A}$ issuing at most q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exists a two-stage algorithm S given uniformly chosen θ such that for any $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$ and any predicate V,*

$$\begin{aligned}&\Pr\Big[(r, m) = (\hat{r}, \hat{m}) \wedge \mathsf{V}(r, m, \theta, z) : (r, m) \leftarrow \mathsf{S}_1^{\mathcal{A}}(), z \leftarrow \mathsf{S}_2^{\mathcal{A}}(\theta)\Big]\\ &\geq \frac{1}{(2q_{\mathsf{qro}} + 1)^2} \Pr\Big[(r, m) = (\hat{r}, \hat{m}) \wedge \mathsf{V}(r, m, \mathsf{H}(r, m), z) : (r, m, z) \leftarrow \mathcal{A}^{|\mathsf{H}\rangle}()\Big].\end{aligned}$$

Semi-classical O2H Technique [1]: We define *punctured oracle* following [12].

Definition 10 (Punctured Oracle [12, Definition 1]). *Let $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$ be a set. Let $\mathsf{f}_{\mathcal{S}} \colon \mathcal{R} \times \mathcal{M} \to \{0, 1\}$ be a predicate that returns 1 if and only if $(r, m) \in \mathcal{S}$.* Punctured oracle *$\mathsf{H}\backslash\mathcal{S}$ (H punctured by $\mathcal{S}$) of $\mathsf{H} \in \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$ runs as follows: on input (r, m), computes whether $(r, m) \in \mathcal{S}$ in an auxilliary qubit $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$, measures $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$, runs $\mathsf{H}(r, m)$, and returns the result. Let* FIND *be an event that any of measurements of $|\mathsf{f}_{\mathcal{S}}(r, m)\rangle$ returns 1.*

The answer from the oracle $\mathsf{H}\backslash\mathcal{S}$ depends on the measurement results. Let us consider a query $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle$. $\mathsf{H}\backslash\mathcal{S}$ computes $\sum_{(r,m)} \alpha_{r,m} |r, m\rangle |y\rangle |\mathsf{f}_{\mathcal{S}}(r, m)\rangle$ and measures the third register. If the result is 0, then the query is transformed to $\sum_{(r,m)\notin\mathcal{S}} \alpha_{r,m} |r, m\rangle |y\rangle |0\rangle$ and $\mathsf{H}\backslash\mathcal{S}$ returns $\sum_{(r,m)\notin\mathcal{S}} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$ to the adversary. If the results is 1 (and thus, $\mathrm{FIND} = \top$ holds), $\mathsf{H}\backslash\mathcal{S}$ returns $\sum_{(r,m)\in\mathcal{S}} \alpha_{r,m} |r, m\rangle |y \oplus \mathsf{H}(r, m)\rangle$ to the adversary. Thus, if $\mathrm{FIND} = \bot$, then the adversary cannot obtain any information on $\mathsf{H}(r, m)$ for $(r, m) \in \mathcal{S}$. Hence, we have the following:

Lemma 3 (Indistinguishability of Punctured Oracles [1, Lemma 1]). *Let $\mathsf{H}_0, \mathsf{H}_1 \colon \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ and $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$, and z be a bitstring. ($\mathcal{S}$, H_0, H_1, and z are taken from arbitrary joint distribution satisfying $\mathsf{H}_0(r, m) = \mathsf{H}_1(r, m)$ for any $(r, m) \notin \mathcal{S}$.) For any quantum adversary $\mathcal{A}$ and any event* E*,*

$$\Pr\Big[\mathrm{E} \wedge \mathrm{FIND} = \bot : b \leftarrow \mathcal{A}^{|\mathsf{H}_0\backslash\mathcal{S}\rangle}(z)\Big] = \Pr\Big[\mathrm{E} \wedge \mathrm{FIND} = \bot : b \leftarrow \mathcal{A}^{|\mathsf{H}_1\backslash\mathcal{S}\rangle}(z)\Big].$$

The following lemma provides a bound on the advantage gap between the original game and a game with a punctured oracle by considering the probability of $\mathrm{FIND} = \top$.

Lemma 4 (Semi-classical O2H Technique [1, Theorem 1]). *Let* $\mathsf{H}\colon \mathcal{R} \times \mathcal{M} \to \mathcal{Y}$ *and* $\mathcal{S} \subset \mathcal{R} \times \mathcal{M}$*, and* z *be a bitstring. (*$\mathcal{S}$*,* H*, and* z *are taken from arbitrary joint distribution.) For any quantum adversary* $\mathcal{A}$ *issuing at most* q_{qro} *(quantum) random oracle queries to* H*,*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}^{|\mathsf{H}\rangle}(z)\right] - \Pr\left[1 \leftarrow \mathcal{A}^{|\mathsf{H}\setminus\mathcal{S}\rangle}(z) \wedge \text{FIND} = \bot\right]\right| \\ \leq \sqrt{(q_{\mathsf{qro}} + 1)\Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}^{|\mathsf{H}\setminus\mathcal{S}\rangle}(z)\right]}.$$

Furthermore, the following provides a bound on $\Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}^{|\mathsf{H}\setminus\mathcal{S}\rangle}(z)\right]$.

Lemma 5 (Search in Semi-classical Oracle [1, Theorem 2 and Corollary 1]). *Let* $\mathcal{A}$ *be a quantum adversary issuing at most* q_{qro} *(quantum) random oracle queries to* H*. Let* $\mathcal{B}^{|\mathsf{H}\rangle}(z)$ *be an algorithm that runs as follows: Picks* $i \leftarrow_{\$} [q_{\mathsf{qro}}]$*, runs* $\mathcal{A}^{|\mathsf{H}\rangle}(z)$ *until just before* i*-th query, measures a query input register in the computational basis, and outputs the measurement outcome as* (r, m)*. Then,*

$$\Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}^{|\mathsf{H}\setminus\mathcal{S}\rangle}(z)\right] \leq 4q_{\mathsf{qro}} \Pr\left[(r, m) \in \mathcal{S} : (r, m) \leftarrow \mathcal{B}^{|\mathsf{H}\rangle}(z)\right].$$

In particular, if for each $(r, m) \in \mathcal{S}$*,* $\Pr[(r, m) \in \mathcal{S}] \leq \epsilon$ *(conditioned on* z*, on other oracles* $\mathcal{A}$ *has access to, and on other outputs of* H*), then*

$$\Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}^{|\mathsf{H}\setminus\mathcal{S}\rangle}(z)\right] \leq 4q_{\mathsf{qro}}\epsilon.$$

3 Existing Security Proofs

We review the existing security proofs, including our own, and summarize them in Table 2.

Security Proof in the ROM [6, 30, 53]: Let $\mathsf{T}_{\mathsf{psf}}$ be a PSF. A reduction of INV ⇒ EUF-CMA of $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$ in the ROM is given by the lazy sampling and programming. The INV adversary $\mathcal{B}_{\mathsf{inv}}$, given a challenge (F, y), simulates the EUF-CMA game played by an adversary $\mathcal{A}_{\mathsf{cma}}$ as follows: For a random oracle query (r, m), $\mathcal{B}_{\mathsf{inv}}$ returns $\mathsf{F}(x)$ for $x \leftarrow \mathsf{SampDom}(\mathsf{F})$ and stores (r, m, x) in a database $\mathcal{D}$. If $(r, m, x) \in \mathcal{D}$ with some x, then $\mathcal{B}_{\mathsf{inv}}$ gives $\mathsf{F}(x)$ to $\mathcal{A}_{\mathsf{cma}}$. For a signing query m, $\mathcal{B}_{\mathsf{inv}}$ chooses (r, x) by $r \leftarrow_{\$} \mathcal{R}$ and $x \leftarrow \mathsf{SampDom}(\mathsf{F})$. If $(r, m, *) \notin \mathcal{D}$, $\mathcal{B}_{\mathsf{inv}}$ returns (r, x) and stores (r, m, x) in $\mathcal{D}$; otherwise $\mathcal{B}_{\mathsf{inv}}$ returns stored (r, x). From **Condition 1** of PSF ($\mathsf{F}(x)$ is uniform), $\mathcal{B}_{\mathsf{inv}}$ can use $\mathsf{F}(x)$ as an output of the random function. Also from **Conditions 2** and **3**, $\mathcal{B}_{\mathsf{inv}}$ can simulate an honestly generated signature $x_i \leftarrow \mathsf{I}(\mathsf{H}(r_i, m_i))$ by $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$. To win the INV game, $\mathcal{B}_{\mathsf{inv}}$ gives his query y to $\mathcal{A}_{\mathsf{cma}}$ in one of $(q_{\mathsf{sign}} + q_{\mathsf{ro}} + 1)$ queries to H. If $\mathcal{A}_{\mathsf{cma}}$ outputs a valid signature (m^*, r^*, x^*) and $\mathsf{H}(r^*, m^*) = y$ holds,

Table 2: Summary of the existing and our security proofs. In "Conditions of PSF", ✓ indicates this condition of PSF (see Definition 6) is necessary, and $\checkmark^1/\checkmark^2$ indicate that **Condition 2** is relaxed as "A bound δ on average of $\delta_{\mathsf{F},\mathsf{I}}$ is negligible" and "$\epsilon_{\mathsf{ps}} = \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$ is negligible". In "Target scheme", $\mathsf{d}/\mathsf{p}/\mathsf{pr}$ stand for the deterministic hash-and-sign, probabilistic hash-and-sign, and probabilistic hash-and-sign with retry.

Security proof	Security Bound	Assumption	Conditions of PSF				Target scheme
			1	2	3	4	
[14]	$\frac{1}{1-2^{-\omega(\log(\lambda))}}\epsilon_{\mathsf{cr}}$	CR	✓	✓	✓	✓	d/p
[61]	$2\sqrt{\left(q_{\mathsf{sign}} + \frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\right)\epsilon_{\mathsf{ow/inv}}}$	OW/INV	✓	✓	✓	–	d/p
ext. of [59]	$4q_{\mathsf{sign}}(q_{\mathsf{qro}} + 1)(2q_{\mathsf{qro}} + 1)^2\epsilon_{\mathsf{ow/inv}}$	OW/INV	✓	✓	✓	–	d/p
[41]	$(2(q_{\mathsf{qro}} + q_{\mathsf{sign}} + 1) + 1)^2\epsilon_{\mathsf{ow/inv}}$	OW/INV	✓	✓	✓	–	d/p
[17]	$\frac{1}{2}\left(\epsilon_{\mathsf{nma}} + \frac{8\pi}{\sqrt{3}}q_{\mathsf{qro}}^{\frac{3}{2}}\sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}\right)\right)$	EUF-NMA	–	$\checkmark^1$	✓	–	p
ours	$(2q_{\mathsf{qro}} + 1)^2\epsilon_{\mathsf{inv}} + \epsilon_{\mathsf{ps}} + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$ $+2(q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}}$	INV	–	$\checkmark^2$	–	–	p/pr
ours	$\epsilon_{\mathsf{nma}} + \epsilon_{\mathsf{ps}} + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$ $+2(q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{\lvert\mathcal{R}\rvert}}$	EUF-NMA	–	$\checkmark^2$	–	–	p/pr
ours	$(2q_{\mathsf{qro}} + 1)^2\epsilon_{\mathsf{ow/inv}} + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{\lvert\mathcal{R}\rvert}}$	OW/INV	✓	✓	✓	–	p

$\mathcal{B}_{\mathsf{inv}}$ can win the INV game by outputting x^*. Since $\mathsf{H}(r^*, m^*) = y$ holds with $\frac{1}{q_{\mathsf{sign}}+q_{\mathsf{ro}}+1}$, we have $\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma^c}}) \leq (q_{\mathsf{sign}} + q_{\mathsf{ro}} + 1)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}})$, where $\mathcal{A}_{\mathsf{cma^c}}$ is an adversary who makes only classical queries[8].

Sakumoto et al. [53] extended the above proof to the probabilistic hash-and-sign with retry assuming non-PSF trapdoor functions. For a random oracle query (r, m), $\mathcal{B}_{\mathsf{inv}}$ returns $y \leftarrow_{\$} \mathcal{Y}$ and saves (r, m, y) in the database $\mathcal{D}'$. For a signing query m_i, $\mathcal{B}_{\mathsf{inv}}$ takes $r_i \leftarrow_{\$} \mathcal{R}$ and $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$. If $(r_i, *, *) \in \mathcal{D}'$, $\mathcal{B}_{\mathsf{inv}}$ aborts the game; otherwise, $\mathcal{B}_{\mathsf{inv}}$ stores $(r_i, m_i, \mathsf{F}(x_i))$ in $\mathcal{D}'$ and outputs (r_i, x_i). There is an issue in the programming $\mathsf{F}(x)$ instead of $y \leftarrow_{\$} \mathcal{Y}$. Since we do not assume **Condition 1** of PSF, $\mathsf{F}(x)$ is not necessarily uniform. Therefore, the output of H becomes biased, and their security proof is flawed.

[8] $\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) = \mathrm{Adv}^{\mathrm{OW}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{ow}})$ holds ($\mathcal{D}_{\mathcal{X}}$ is defined as $\mathsf{SampDom}(\mathsf{F})$ in the OW game (see Fig. 3)) since the OW adversary can simulate the INV game by giving a uniform $y = \mathsf{F}(x)$ to the INV adversary, and vice versa.

Security Proof by Semi-constant Distribution [61]: Zhandry showed the reduction from the OW assumption of trapdoor permutation in the QROM using a technique called *semi-constant distribution*, which leads to a reduction from the INV assumption of PSF. $\mathcal{B}_{\mathsf{inv}}$ simulates the EUF-CMA game by generating signatures without the trapdoor as the above security proof in the ROM. Instead of adaptively programming H, $\mathcal{B}_{\mathsf{inv}}$ replaces H as $\mathsf{H}' = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r, m)))$, where $\mathsf{DetSampDom}$ is a deterministic function of $\mathsf{SampDom}$ and $\widetilde{\mathsf{H}} \leftarrow_{\$} \mathcal{W}^{\mathcal{R}\times\mathcal{M}}$ is a random function to output randomness for $\mathsf{DetSampDom}$ [14]. From **Condition 1**, H' is indistinguishable from H.

The INV adversary $\mathcal{B}_{\mathsf{inv}}$ programs H' that outputs y with probability ϵ (semi-constant distribution). In the signing oracle, if $\mathsf{H}'(r_i, m_i)$ outputs y, $\mathcal{B}_{\mathsf{inv}}$ aborts this game. A bound on the statistical distance between the random function and the programmed one with the semi-constant distribution is $\frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\epsilon^2$ [61, Corollary 4.3]. When $\mathcal{A}_{\mathsf{cma}}$ wins the EUF-CMA game, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game with probability $(1-\epsilon)^{q_{\mathsf{sign}}}\epsilon \approx \epsilon - q_{\mathsf{sign}}\epsilon^2$. Minimizing the bound $\frac{1}{\epsilon}\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}} + \left(q_{\mathsf{sign}} + \frac{8}{3}(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)^4\right)\epsilon$ gives [61, Theorem 5.3]

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 2\sqrt{\left(q_{\mathsf{sign}} + \frac{8}{3}\left(q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1\right)^4\right)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}})}.$$

Application of Lifting Theorem [59]: Yamakawa and Zhandry gave the lifting theorem for search-type games. As an application of the lifting theorem, they showed $\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma}}) \leq (2q_{\mathsf{qro}} + 1)^2\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma^c}})$, where $\mathcal{A}_{\mathsf{nma^c}}$ is an EUF-NMA adversary making classical queries to H [59, Corollary 4.10]. For a hash-and-sign signature $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}]$, they showed $\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 4q_{\mathsf{sign}}\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ [59, Theorem 4.11]. Extending the results of [59] using the security proof in the ROM, we have a bound:

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq 4q_{\mathsf{sign}}(q_{\mathsf{qro}} + 1)(2q_{\mathsf{qro}} + 1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}).$$

Reduction from EUF-NMA *for WPSF [17]:* The security proofs mentioned above hold only if the underlying trapdoor function is PSF. To relax the conditions on trapdoor functions, Chailloux and Debris-Alazard gave EUF-NMA ⇒ EUF-CMA for the probabilistic hash-and-sign[9]. The authors assumed a WPSF with **Condition 3** and a weaker version of **Condition 2**, that is, there is a bound δ on the average of statistical distance $\delta_{\mathsf{F},\mathsf{I}} = \Delta(\mathsf{SampDom}(\mathsf{F}), \mathsf{I}(\mathsf{U}(\mathcal{Y})))$ over all $(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$. Let $\mathsf{T}_{\mathsf{wpsf}}$ be a WPSF. The EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ replaces the random function H by H', which outputs $\mathsf{H}(r, m)$ with probability $\frac{1}{2}$ and $\mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, w))$ with probability $\frac{1}{2}$. A bound on the advantage of

[9] The authors of [17] defined a problem called *claw with random function problem*; however, its definition is identical to EUF-NMA game for hash-and-sign.

distinguishing H from H' is $\frac{8\pi}{\sqrt{3}} q_{\mathsf{qro}}^{3/2}\sqrt{\delta}$. The authors gave [17, Theorem 2]

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{2}\left(\mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \frac{8\pi}{\sqrt{3}} q_{\mathsf{qro}}^{\frac{3}{2}}\sqrt{\delta} + q_{\mathsf{sign}}\left(\delta + \frac{q_{\mathsf{sign}}}{|\mathcal{R}|}\right)\right). \tag{1}$$

Reduction from Collision-resistance [14]: Boneh et al. [14] gave a reduction from the CR of a PSF $\mathsf{T}_{\mathsf{psf}}$ to the sEUF-CMA security of $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]$. The CR adversary $\mathcal{B}_{\mathsf{cr}}$ given F simulates the sEUF-CMA game for $\mathcal{A}_{\mathsf{cma}}$. For a random function $\widetilde{\mathsf{H}} \leftarrow_{\$} \mathcal{W}^{\mathcal{R}\times\mathcal{M}}$, $\mathcal{B}_{\mathsf{cr}}$ replaces H as $\mathsf{H}'(r,m) = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r,m)))$, where H and H' are indistinguishable from **Condition 1**. Also, $\mathcal{B}_{\mathsf{cr}}$ simulates the signing oracle using **Conditions 2** and **3**. If $\mathcal{A}_{\mathsf{cma}}$ wins, then $\mathsf{F}(x^*) = \mathsf{H}'(r^*,m^*) = \mathsf{F}(x')$ holds for $x' = \mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(r^*,m^*))$. When $x^* \neq x'$, $\mathcal{B}_{\mathsf{cr}}$ can obtain a collision pair (x^*, x'). Since $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log(\lambda))}$ (see **Condition 4**),

$$\mathrm{Adv}^{\text{sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1-2^{-\omega(\log(\lambda))}}\mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}}). \tag{2}$$

Concurrent Work [41]: Liu, Jiang, and Zhao [41] showed OW ⇒ EUF-CMA for the deterministic/probabilistic hash-and-sign based on trapdoor permutations in the QROM. Their reduction can be extended to INV ⇒ EUF-CMA for the deterministic/probabilistic hash-and-sign based on PSFs. As in [18, 14, 61], the random function H is replaced as $\mathsf{H}' = \mathsf{F}(\mathsf{DetSampDom}(\mathsf{F}, \widetilde{\mathsf{H}}(m)))$ to answer the signing queries without using the trapdoor. From **Condition 1**, this modification does not incur any security loss. Then, their reduction uses the measure-and-reprogram technique [23, Theorem 2] (see Lemma 2 in Section 2.7) as in our security proof. Their reduction has a security bound that includes q_{sign} in the multiplicative loss:[10]

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2(q_{\mathsf{qro}} + q_{\mathsf{sign}} + 1) + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{A}_{\mathsf{inv}}). \tag{3}$$

4 New Security Proof

The main theorem is as follows:

Theorem 1 (INV ⇒ EUF-CMA (Main Theorem)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exist an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *and a* PS *adversary* $\mathcal{D}_{\mathsf{ps}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *issuing* q_{sign} *sampling queries such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}, \tag{4}$$

[10] In the latest version of [41], a term q_{sign} has been removed from Eq. (3); however, we have identified a flaw in the proof (see Appendix A).

where q'_{sign} is a bound on the total number of queries to H in all the signing queries, and the running times of $\mathcal{B}_{\mathsf{inv}}$ and $\mathcal{D}_{\mathsf{ps}}$ are about that of $\mathcal{A}_{\mathsf{cma}}$.

If $\mathcal{A}_{\mathsf{cma}}$ makes only classical random oracle queries q_{ro} times, then

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \le (q_{\mathsf{ro}}+1)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) + q'_{\mathsf{sign}}\frac{q'_{\mathsf{sign}}+q_{\mathsf{ro}}+1}{|\mathcal{R}|} + (q_{\mathsf{ro}}+1)\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}.$$

Proof. In the beginning, we show that we can set q'_{sign} as $q'_{\mathsf{sign}} = \frac{c}{\rho}q_{\mathsf{sign}}$ for some constant $c > 1$, where $\rho = \Pr[x \ne \bot : y \leftarrow_{\$} \mathcal{Y}, x \leftarrow \mathsf{I}(y)]$. In q'_{sign} trials, at least q_{sign} signatures are generated if the number of successful trials (where $\mathsf{I}(\mathsf{H}(r,m))$ outputs a preimage) is q_{sign} or more. Let S be a random variable for the number of successful trials. $\mathbb{E}(S) = \rho q'_{\mathsf{sign}} = c q_{\mathsf{sign}}$ holds. From the Chernoff bound, we have $\Pr[S \le (1-\gamma)\mathbb{E}(S)] \le e^{-\frac{1}{2}\gamma^2\mathbb{E}(S)}$. Substituting $\gamma = \frac{\mathbb{E}(S)-q_{\mathsf{sign}}+1}{\mathbb{E}(S)}$, the LHS becomes $\Pr[S \le q_{\mathsf{sign}}-1]$ that is a probability that we cannot generate q_{sign} signatures with q'_{sign} trials. Since we set $q'_{\mathsf{sign}} = \frac{c}{\rho}q_{\mathsf{sign}}$, the exponent of the RHS becomes $-\frac{((c-1)q_{\mathsf{sign}}+1)^2}{2cq_{\mathsf{sign}}} \ge -\frac{c-1}{2c}q_{\mathsf{sign}}$ and the bound on $\Pr[S \le q_{\mathsf{sign}}-1]$ becomes negligible for $q_{\mathsf{sign}} = \omega(\log(\lambda))$.

In the upcoming proof, we will explain the proofs in parallel for both the ROM and QROM. For the figures, we will use notations assuming the QROM.

EUF-NMA ⇒ EUF-CMA*:* Figs. 9 and 10 show the games and simulations described below. Without loss of generality, we assume that $\mathcal{A}_{\mathsf{cma}}$ makes a query (r^*, m^*) (the final ouput) to H. Then, the total number of queries to H is $q_{\mathsf{ro}}+1$ (classical) or $q_{\mathsf{qro}}+1$ (quantum).

Game G_0 (EUF-CMA game): This is the original EUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}})$ holds.

Game G_1 (adaptive reprogramming of H): The signing oracle $\mathsf{Sign}^{\mathsf{H}}$ uniformly chooses y_i and reprograms $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$ until $\mathsf{I}(y_i)$ does not output $\bot$ (see Lines 3 to 5 in $\mathsf{Sign}^{\mathsf{H}}$ for G_1). Considering the number of retries, H is reprogrammed for at most q'_{sign} times.

ROM: When the signing oracle has not chosen the same r_i in Line 2 of $\mathsf{Sign}^{\mathsf{H}}$ more than twice, and the chosen r_i has not been queried to H in advance, there is no difference in the advantages between G_0 and G_1. Therefore, $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \le q'_{\mathsf{sign}}\frac{q'_{\mathsf{sign}}+q_{\mathsf{ro}}+1}{|\mathcal{R}|}$ holds.

QROM: The AR adversary $\mathcal{D}_{\mathsf{ar}}$ can simulate $\mathsf{G}_0/\mathsf{G}_1$ (the top row of Fig. 10). If $\mathcal{D}_{\mathsf{ar}}$ plays AR_0, $\mathcal{D}_{\mathsf{ar}}$ simulates G_0; otherwise it simulates G_1. From Lemma 1, we have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \le \mathrm{Adv}^{\mathrm{AR}}_{\mathsf{H}}(\mathcal{D}_{\mathsf{ar}}) \le \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}}$.

Game G_2 (pre-choosing r for unsuccessful trials): In the beginning, the challenger chooses $r \leftarrow_{\$} \mathcal{R}$ for $q'_{\mathsf{sign}} - q_{\mathsf{sign}}$ times and keeps them in a sequence $\mathcal{S}$ (elements of $\mathcal{S}$ are ordered and may be duplicated.). In the signing oracle, $r_i = \mathcal{S}[ctr]$ is used for reprogramming if $\mathsf{I}(y_i)$ outputs $\bot$ for $y_i \leftarrow_{\$} \mathcal{Y}$ (see

```
GAME: $\mathsf{G}_0$-$\mathsf{G}_1$
1  $\mathcal{Q} := \emptyset$
2  $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3  $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
4  $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\rangle}(\mathsf{F})$
5  if $m^* \in \mathcal{Q}$ then
6      return $0$
7  return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}(r^*, m^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_0$
1  repeat
2      $r_i \leftarrow_\$ \mathcal{R}$
3      $x_i \leftarrow \mathsf{I}(\mathsf{H}(r_i, m_i))$
4  until $x_i \neq \bot$
5  $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
6  return $(r_i, x_i)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_1$
1  repeat
2      $r_i \leftarrow_\$ \mathcal{R}$
3      $y_i \leftarrow_\$ \mathcal{Y}$
4      $x_i \leftarrow \mathsf{I}(y_i)$
5      $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
6  until $x_i \neq \bot$
7  $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
8  return $(r_i, x_i)$
```

```
GAME: $\mathsf{G}_2$
1  $\mathcal{Q} := \emptyset$
2  $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3  $ctr := 0$
4  $\mathcal{S} := \emptyset$
5  for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ do
6      $r \leftarrow_\$ \mathcal{R}$
7      $\mathcal{S} := \mathcal{S} \cup \{r\}$
8  $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
9  $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\rangle}(\mathsf{F})$
10 if $m^* \in \mathcal{Q}$ then
11     return $0$
12 return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}(r^*, m^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_2$
1  repeat
2      $y_i \leftarrow_\$ \mathcal{Y}$
3      $x_i \leftarrow \mathsf{I}(y_i)$
4      if $x_i = \bot$ then
5          $ctr := ctr + 1$
6          $r_i := \mathcal{S}[ctr]$
7      else
8          $r_i \leftarrow_\$ \mathcal{R}$
9      $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
10 until $x_i \neq \bot$
11 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
12 return $(r_i, x_i)$
```

```
GAME: $\mathsf{G}_3$-$\mathsf{G}_5$
1  $\mathcal{Q} := \emptyset$
2  $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
3  $\mathrm{FIND} := \bot$
4  $ctr := 0$
5  $\mathcal{S} := \emptyset$
6  for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ do
7      $r \leftarrow_\$ \mathcal{R}$
8      $\mathcal{S} := \mathcal{S} \cup \{r\}$
9  $\mathcal{S}' := \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$
10 $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
11 $(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\setminus\mathcal{S}'\rangle}(\mathsf{F})$
12 if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ then
13     return $0$
14 return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}(r^*, m^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_3$
1  repeat
2      $y_i \leftarrow_\$ \mathcal{Y}$
3      $x_i \leftarrow \mathsf{I}(y_i)$
4      if $x_i = \bot$ then
5          $ctr := ctr + 1$
6          $r_i := \mathcal{S}[ctr]$
7      else
8          $r_i \leftarrow_\$ \mathcal{R}$
9      $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
10 until $x_i \neq \bot$
11 $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
12 return $(r_i, x_i)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_4$
1  repeat
2      $y_i \leftarrow_\$ \mathcal{Y}$
3      $x_i \leftarrow \mathsf{I}(y_i)$
4  until $x_i \neq \bot$
5  $r_i \leftarrow_\$ \mathcal{R}$
6  $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
7  $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
8  return $(r_i, x_i)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_5$
1  $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
2  $r_i \leftarrow \mathcal{R}$
3  $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto \mathsf{F}(x_i)}$
4  $\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
5  return $(r_i, x_i)$
```

Fig. 9: Games for EUF-NMA ⇒ EUF-CMA. The modifications from the previous game are highlighted in red text.

Lines 6 and 9 of $\mathsf{Sign}^{\mathsf{H}}$ for G_2), where $\mathcal{S}[j]$ is j-th element of $\mathcal{S}$ and ctr is a counter that increments just before using $\mathcal{S}[ctr]$.

ROM and QROM: In G_1, the challenger can choose r_i in the beginning since r_i is chosen independently of m_i queried by $\mathcal{A}_{\mathsf{cma}}$. Also, r_i is always uniformly chosen whatever $\mathsf{I}(y_i)$ outputs. Therefore, the challenger can use r_i chosen in the beginning only when $\mathsf{I}(y)$ outputs $\bot$. Hence, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds.

$\mathcal{D}_{\mathsf{ar}}^{|\mathsf{H}_b\rangle}()$ simulates $\mathsf{G}_0/\mathsf{G}_1$

```
$\mathcal{Q} := \emptyset$
$(\mathsf{F}, \mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}_b\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q}$ then
    return $0$
return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}_b(r^*, m^*)$
```

$\mathsf{Sign}^{\mathsf{H}_b, \mathsf{Repro}}(m_i)$

```
repeat
    $r_i \leftarrow \mathsf{Repro}(m_i)$
    $x_i \leftarrow \mathsf{I}(\mathsf{H}_b(r_i, m_i))$
until $x_i \neq \bot$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(r_i, x_i)$
```

$\mathcal{D}_{\mathsf{ps}}^{\mathsf{Sample}_b}(\mathsf{F})$ simulates $\mathsf{G}_4/\mathsf{G}_5$

```
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$
$\mathrm{FIND} := \bot$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ do
    $r \leftarrow_\$ \mathcal{R}$
    $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' := \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \backslash \mathcal{S}'\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ then
    return $0$
return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}(r^*, m^*)$
```

$\mathsf{Sign}^{\mathsf{H}, \mathsf{Sample}_b}(m_i)$

```
$x_i \leftarrow \mathsf{Sample}_b()$
$r_i \leftarrow_\$ \mathcal{R}$
$\mathsf{H} := \mathsf{H}^{(r_i, m_i) \mapsto \mathsf{F}(x_i)}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(r_i, x_i)$
```

$\mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})$ simulates G_5

```
$\mathcal{Q} := \emptyset$
$\mathsf{H}' := \mathsf{H}$
$\mathrm{FIND} := \bot$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}} - q_{\mathsf{sign}}]$ do
    $r \leftarrow_\$ \mathcal{R}$
    $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' := \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$
$(m^*, r^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}' \backslash \mathcal{S}'\rangle}(\mathsf{F})$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ then
    return $0$
return $\mathsf{F}(x^*) \overset{?}{=} \mathsf{H}'(r^*, m^*)$
```

$\mathsf{Sign}^{\mathsf{H}'}(m_i)$

```
$x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$
$r_i \leftarrow_\$ \mathcal{R}$
$\mathsf{H}' := \mathsf{H}'^{(r_i, m_i) \mapsto \mathsf{F}(x_i)}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(r_i, x_i)$
```

Fig. 10: Simulations for EUF-NMA ⇒ EUF-CMA

Game G_3 (puncturing H): Let $\mathcal{S}' = \{(r, m) : r \in \mathcal{S}, m \in \mathcal{M}\}$ be a set induced by $\mathcal{S}$. Instead of H, $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H} \backslash \mathcal{S}'$ (H punctured by $\mathcal{S}'$). Also, G_3 outputs 0 if $\mathrm{FIND} = \top$ (see the definitions of $\mathsf{H} \backslash \mathcal{S}'$ and FIND in Definition 10).

ROM: Since $\mathsf{H} \backslash \mathcal{S}'$ is purely classical, FIND becomes $\top$ with at most $(q_{\mathsf{ro}} + 1)\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$; therefore, $\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq (q_{\mathsf{ro}} + 1)\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds.

QROM: We use Lemma 4 to bound $\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right|$. Suppose that $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(\mathsf{F})\right]$. Since G_3 uses $\mathsf{H} \backslash \mathcal{S}'$ and outputs 0 if $\mathrm{FIND} = \top$, we have $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \backslash \mathcal{S}'\rangle}(\mathsf{F}) \wedge \mathrm{FIND} = \bot\right]$

```
GAME: $\mathsf{G}_4'$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$
$\mathcal{S} := \emptyset$
for $j \in [q'_{\mathsf{sign}}]$ do
    $r \leftarrow_\$ \mathcal{R}$
    $\mathcal{S} := \mathcal{S} \cup \{r\}$
$\mathcal{S}' = \{(r,m) : r \in \mathcal{S}, m \in \mathcal{M}\}$
$(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$
$(r',m') \leftarrow \mathcal{B}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\rangle}(\mathsf{F})$
return $(r',m') \overset{?}{\in} \mathcal{S}'$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_4'$
repeat
    $y_i \leftarrow_\$ \mathcal{Y}$
    $x_i \leftarrow \mathsf{I}(y_i)$
until $x_i \neq \perp$
$r_i \leftarrow_\$ \mathcal{R}$
$\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(r_i, x_i)$
```

Fig. 11: A game G_4' used in the application of Lemma 5

and $\Pr\left[\text{FIND} = \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\backslash\mathcal{S}'\rangle}(\mathsf{F})\right]$. Then,

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \sqrt{(q_{\mathsf{qro}}+2)\Pr\left[\text{FIND} = \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]}, \quad (5)$$

by Lemma 4. We will show a bound on Eq. (5) after defining G_4.

GAME G_4 (reprogramming only for successful trials): The signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(r_i,m_i)\mapsto y_i}$ only for $r_i \leftarrow \mathcal{R}$, $y_i \leftarrow_\$ \mathcal{Y}$, and $x_i \leftarrow \mathsf{I}(y_i)$ satisfying $x_i \neq \perp$. Notice that $\mathcal{A}_{\mathsf{cma}}$ makes queries to the punctured oracle $\mathsf{H}\backslash\mathcal{S}'$.

ROM: Since $\mathcal{A}_{\mathsf{cma}}$ cannot distinguish whether H is reprogrammed for $(r,m) \in \mathcal{S}'$ if FIND $= \perp$, $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds.

QROM: If the measurements of $|\mathsf{f}_{\mathcal{S}'}(r,m)\rangle$ are 0 for all queries (FIND $= \perp$), then $\mathcal{A}_{\mathsf{cma}}$'s queries never contain any $(r,m) \in \mathcal{S}'$ and $\mathcal{A}_{\mathsf{cma}}$ cannot obtain $\mathsf{H}(r,m)$ for $(r,m) \in \mathcal{S}'$. Hence, if FIND $= \perp$, then $\mathcal{A}_{\mathsf{cma}}$ cannot distinguish whether H is reprogrammed at $(r,m) \in \mathcal{S}'$ in G_3 or not in G_4 and we have

$$\Pr\left[\text{FIND} = \perp : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\text{FIND} = \perp : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \quad (6)$$

(as Lemma 3). Especially, if G_3 or G_4 outputs 1, then FIND should be $\perp$ (Line 12 of G_3-G_5). Thus, $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. Moreover, $\Pr\left[\text{FIND} = \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\text{FIND} = \top : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]$ holds from Eq. (6).

Let G_4' be a game given in Fig. 11 (identical to G_4 except that $\mathcal{B}_{\mathsf{cma}}$ outputs (r',m') and H is not punctured). Choosing $j \leftarrow_\$ [q_{\mathsf{qro}}+1]$, $\mathcal{B}_{\mathsf{cma}}$ runs $\mathcal{A}_{\mathsf{cma}}$ playing G_4. Just before $\mathcal{A}_{\mathsf{cma}}$ makes j-th query to H, $\mathcal{B}_{\mathsf{cma}}$ measures a query input register of $\mathcal{A}_{\mathsf{cma}}$ and outputs the measurement outcome as (r',m'). Since the oracles of G_4' reveal no information on $\mathcal{S}$, $\mathcal{B}_{\mathsf{cma}}$ has no information on $\mathcal{S}$; therefore, $\Pr\left[\mathsf{G}_4'^{\mathcal{B}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \Pr[r' \in \mathcal{S}] \leq \frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds. Hence, $\Pr\left[\text{FIND} = \top : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \leq 4(q_{\mathsf{qro}}+1)\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}$ holds from Lemma 5 and an upper bound on Eq. (5) is $2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}$.

GAME G_5 (simulating the signing oracle by $\mathsf{SampDom}$): The signing oracle generates signatures by $r_i \leftarrow_\$ \mathcal{R}$ and $x_i \leftarrow \mathsf{SampDom}(\mathsf{F})$.

ROM and QROM: The PS adversary $\mathcal{D}_{\mathsf{ps}}$ can simulate $\mathsf{G}_4/\mathsf{G}_5$ as in the second row of Fig. 10. If $\mathcal{D}_{\mathsf{ps}}$ plays PS_0, the procedures of the original and simulated G_4 are identical. If $\mathcal{D}_{\mathsf{ps}}$ plays PS_1, he simulates G_5. Thus, we have $\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}})$.

We show that the EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ can simulate G_5 as in the bottom row of Fig. 10. In the simulation, $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H}' \backslash \mathcal{S}'$, where H' outputs whatever H outputs except for $\{(r_i, m_i)\}_{i \in [q_{\mathsf{sign}}]}$. Since $m^* \notin \mathcal{Q}$ holds if $\mathcal{A}_{\mathsf{cma}}$ wins, $\mathsf{H}'(r^*, m^*) = \mathsf{H}(r^*, m^*)$ holds for (m^*, r^*, x^*) that $\mathcal{A}_{\mathsf{cma}}$ returns. Therefore, $\mathcal{A}_{\mathsf{nma}}$ wins his game if $\mathcal{A}_{\mathsf{cma}}$ wins the EUF-CMA game. Hence, $\mathcal{A}_{\mathsf{nma}}$ can perfectly simulate G_5 with the same number of queries and almost the same running time as $\mathcal{A}_{\mathsf{cma}}$, and $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds. We finally stress that the number of queries $\mathcal{A}_{\mathsf{nma}}$ made to H is q_{qro} rather than $q_{\mathsf{qro}} + q_{\mathsf{sign}}$ since $\mathcal{A}_{\mathsf{nma}}$ never queries to its random oracle in the simulation of the signature.

Summing up, we have

$$\begin{aligned}\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\leq \mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) \\ &\quad + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}. \end{aligned} \tag{7}$$

INV ⇒ EUF-NMA*:* We use different techniques for the ROM and the QROM.

ROM: Given a challenge y, the INV adversary $\mathcal{B}_{\mathsf{inv}}$ randomly picks one of queries to H and reprograms H and $\mathsf{H}^{(r,m)\mapsto y}$. If $\mathcal{A}_{\mathsf{nma}}$ wins his game with (m^*, r^*, x^*) and $\mathsf{H}(r^*, m^*) = y$ holds, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game with x^*. Since $\mathsf{H}(r^*, m^*) = y$ holds with probability $\frac{1}{q_{\mathsf{ro}}+1}$, $\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) \leq (q_{\mathsf{ro}} + 1)\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}})$.

QROM: We use Lemma 2. Let S be a two-stage algorithm that consists of S_1 and S_2 and runs $\mathcal{A}_{\mathsf{nma}}$ in the EUF-NMA game as follows:

1. Choose $(i, b) \leftarrow_{\$} ([q_{\mathsf{qro}}] \times \{0, 1\}) \cup \{(q_{\mathsf{qro}} + 1, 0)\}$.
2. Run $\mathcal{A}_{\mathsf{nma}}$ with H until i-th query.
3. Measure i-th query and output (r, m) as the output of S_1.
4. Given a random θ, reprogram $\mathsf{H}' = \mathsf{H}^{(r,m)\mapsto\theta}$.
5. If $i = q_{\mathsf{qro}} + 1$, then go to Step 8.
6. Answer i-th query with H (if $b = 0$) or H' (if $b = 1$).
7. Run $\mathcal{A}_{\mathsf{nma}}$ with H' until the end.
8. Output $\mathcal{A}_{\mathsf{nma}}$'s output (m^*, r^*, x^*) as the output of S_2.

The INV adversary $\mathcal{B}_{\mathsf{inv}}$ runs S. Since y is uniform in the INV game, $\mathcal{B}_{\mathsf{inv}}$ can set the input for S_2 as $\theta \coloneqq y$. When the predicate is $\mathsf{F}(x) \overset{?}{=} \mathsf{H}(r, m)$, we have

$$\begin{aligned}&\Pr\left[(r, m) = (\hat{r}, \hat{m}) \wedge \mathsf{F}(x) = y : (r, m) \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}}(), (m, r, x) \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}}(y)\right] \\ \geq &\frac{1}{(2q_{\mathsf{qro}} + 1)^2} \Pr\left[(r, m) = (\hat{r}, \hat{m}) \wedge \mathsf{F}(x) = \mathsf{H}(r, m) : (m, r, x) \leftarrow \mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})\right],\end{aligned}$$

for any $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$ from Lemma 2. By summing over all $(\hat{r}, \hat{m}) \in \mathcal{R} \times \mathcal{M}$,

$$\begin{aligned}&\Pr\Big[\mathsf{F}(x) = y : (r, m) \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}}(), (m, r, x) \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}}(y)\Big] \\ &\qquad \geq \frac{1}{(2q_{\mathsf{qro}} + 1)^2} \Pr\Big[\mathsf{F}(x) = \mathsf{H}(r, m) : (m, r, x) \leftarrow \mathcal{A}_{\mathsf{nma}}^{|\mathsf{H}\rangle}(\mathsf{F})\Big]. \quad (8)\end{aligned}$$

Notice that the probability in the RHS of Eq. (8) is the EUF-NMA advantage. Also, $\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) \geq \Pr\Big[\mathsf{F}(x) = y : (r, m) \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{nma}}}(), (m, r, x) \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{nma}}}(y)\Big]$ holds since $\mathcal{B}_{\mathsf{inv}}$ runs S. Hence, we have

$$\mathrm{Adv}^{\mathrm{EUF\text{-}NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) \leq (2q_{\mathsf{qro}} + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}). \quad (9)$$

From Eqs. (7) and (9), we have Eq. (4). □

Theorem 1 has the following two advantages:

Advantage 1 (Wide applications): Our reduction gives security proofs for code-based and MQ-based hash-and-sign signatures. Relaxation of **Condition 2** is necessary for such applications. The existing security proofs replace the random function H with H' all at once, requiring statistical indistinguishability between H and H'. On the other hand, our proof adaptively reprograms H in each signing query. This approach enables us to provide the security proof under a weaker assumption compared to the one required by PSF, namely, a trapdoor function is WPSF and preimage-simulatable. When considering the PS advantage, the use of computational indistinguishability leads to further relaxation of requirements for the trapdoor function.

Advantage 2 (Tighter proof): Our reduction is tighter than the existing ones [61, 59]. While we cannot guarantee the optimality of our reduction, we can infer from several observations that a multiplicative loss of $(2q_{\mathsf{qro}} + 1)^2$ appears to be unavoidable in the generic (black-box) reduction. The reduction incurs a loss of the number of queries to H, even in the ROM (see Section 3). Second, the security loss of a generic reduction from ROM to QROM using the lifting theorem [59] is at least $(2q_{\mathsf{qro}} + 1)^2$. Third, in the Fiat-Shamir paradigm, a generic reduction from arbitrary ID schemes incurs the same security loss (see Remark 4).

We give some remarks on Theorem 1.

Remark 1. If $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}]$ adopts the probabilistic hash-and-sign, then $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds and the last term of Eq. (4) becomes 0.

Remark 2. We have a tight reduction in EUF-NMA ⇒ EUF-CMA with the security bound of Eq. (7). Comparing this bound with the one presented in [17] (refer to Eq. (1) in Section 3), we observe that our requirement for $\mathsf{T}_{\mathsf{wpsf}}$ is weaker, and there are no square-root terms associated with **Condition 2**.

Remark 3. When the underlying trapdoor function is PSF (or trapdoor permutation), we have:

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}}.$$

As $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}].\mathsf{Sign}$ produces a signature without retry (**Condition 3**), $q'_{\mathsf{sign}} = q_{\mathsf{sign}}$ holds. In the PS game, the outputs of I and $\mathsf{SampDom}(\mathsf{F})$ are equivalent due to **Condition 2**, resulting in $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{D}_{\mathsf{ps}}) = 0$. This bound is tighter than existing ones for $\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]$ (see Table 2).

Remark 4. Grilo et al. showed a tight reduction of EUF-NMA ⇒ EUF-CMA in the Fiat-Shamir paradigm, assuming that the underlying ID scheme is honest verifier zero-knowledge (HVZK) [32, Theorem 3]. Also, Don et al. gave a generic reduction in the Fiat-Shamir transform of arbitrary ID schemes with a security loss $(2q_{\mathsf{qro}}+1)^2$ [24, Theorem 8]. The above reductions use the tight adaptive reprogramming technique and the measure-and-reprogram technique.

4.1 Extension to sEUF-CMA Security

If F is injective, $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]$ is sEUF-CMA secure.

Corollary 1 (INV ⇒ sEUF-CMA). *Suppose that F of $\mathsf{T}_{\mathsf{wpsf}}$ is an injection. For any quantum* sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ and a* PS *adversary $\mathcal{D}_{\mathsf{ps}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ issuing q_{sign} sampling queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}}) \\ &+\frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}, \end{aligned} \tag{10}$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries, and the running times of $\mathcal{B}_{\mathsf{inv}}$ and $\mathcal{D}_{\mathsf{ps}}$ are about that of $\mathcal{A}_{\mathsf{cma}}$.

Proof. The sEUF-CMA game outputs 0 if $(m^*, r^*, x^*) \in \mathcal{Q}'$. Due to the injection of F, if $(m^*, r^*) = (m_i, r_i)$, it implies $x^* = x_i$. Therefore, we can rephrase the condition for outputting 0 as follows: the game outputs 0 if $(m^*, r^*) \in \mathcal{Q}'$, where $\mathcal{Q}' = \{(m_i, r_i)\}_{i\in[q_{\mathsf{sign}}]}$. With this reinterpretation, we demonstrate that the same bound as Eq. (7) holds for EUF-NMA ⇒ sEUF-CMA.

In Corollary 1, we can use the same games as defined in Theorem 1, and the bound on $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right|$ remains unchanged. In the simulation of G_5 (see the bottom row of Fig. 10), $\mathcal{A}_{\mathsf{cma}}$ uses $\mathsf{H}'\backslash\mathcal{S}'$ reprogrammed on $\{(r_i, m_i)\}_{i\in[q_{\mathsf{sign}}]}$ instead of the original H. By $(m^*, r^*) \notin \mathcal{Q}'$, $\mathsf{H}'(r^*, m^*) = \mathsf{H}(r^*, m^*)$ holds and $\mathcal{A}_{\mathsf{nma}}$ can win his game if $\mathsf{F}(x^*) = \mathsf{H}'(r^*, m^*)$. Therefore, $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds. Hence, Eq. (7) holds. □

4.2 Applications of New Security Proof

By applying Theorem 1, we can establish security proofs for Wave [2], the original/modified UOV signatures [39, 53], the modified HFE signature [53], and MAYO [10]. Additionally, by utilizing Corollary 1, we can provide a security proof for the modified CFS signature [20]. Essentially, it is sufficient to directly apply Theorem 1 or Corollary 1; however, we need to derive bounds on the PS advantage, denoted by ϵ_{ps}. We briefly explain ideas behind bounding ϵ_{ps} (see the complete proofs in Appendix B).

Modified CFS signature: An invertible subset of $\mathcal{Y}$, that is, $\mathcal{Y}' = \{y : \mathsf{I}(y) \neq \perp\}$, is a set of decodable syndromes of a Goppa code and the domain $\mathcal{X}$ of F is a set of corresponding errors. Given the relationship between $\mathcal{X}$ and $\mathcal{Y}'$, there exists a one-to-one correspondence between $x \in \mathcal{X}$ and $y \in \mathcal{Y}'$, and consequently, F is an injection (Corollary 1 is applied). Therefore, a preimage generated after retries is uniform over $\mathcal{X}$, and thus, $\mathsf{SampDom}(\mathsf{F})$, that is, $x \leftarrow_{\$} \mathcal{X}$, can perfectly simulate the preimage. Hence, $\epsilon_{\mathsf{ps}} = 0$ holds.

Wave: Wave adopts the probabilistic hash-and-sign (Eq. (7) is applied.) and its trapdoor function is *average trapdoor PSF (ATPSF)* [17] that is a special case of WPSF satisfying:

1. There is a bound δ on the average of $\delta_{\mathsf{F},\mathsf{I}}$ over all $(\mathsf{F},\mathsf{I}) \leftarrow \mathsf{Gen}(1^\lambda)$, where $\delta_{\mathsf{F},\mathsf{I}} = \Delta(\mathsf{SampDom}(\mathsf{F}), \mathsf{I}(\mathsf{U}(\mathcal{Y})))$ is a statistical distance between $\mathsf{SampDom}(\mathsf{F})$ and $\mathsf{I}(y)$ for $y \leftarrow_{\$} \mathcal{Y}$ (**relaxed Condition 2**).
2. $\mathsf{I}(y)$ outputs x satisfying $\mathsf{F}(x) = y$ for any $y \in \mathcal{Y}$ (**Condition 3**).

Applying the union bound over q_{sign} signing queries, we have $\epsilon_{\mathsf{ps}} \leq q_{\mathsf{sign}}\delta$.

Original UOV signature: Since there is no known statistical bound on ϵ_{ps}, we must assume the computational hardness of the PS game.

Modified UOV/HFE signatures: Since a preimage generated after retries follows a uniform distribution as shown in [53], $x \leftarrow \mathsf{SampDom}(\mathsf{F})$, that is, $x \leftarrow_{\$} \mathcal{X}$, can perfectly simulate the preimage; therefore, we have $\epsilon_{\mathsf{ps}} = 0$.

MAYO: MAYO adopts the probabilistic hash-and-sign (Eq. (7) is applied.) and its trapdoor I iteratively retries a part of x called *vinegar variables* until a specific condition is met. If I consistently outputs x without needing to retry the vinegar variables, then $\mathsf{SampDom}(\mathsf{F})$ ($x \leftarrow_{\$} \mathcal{X}$) can perfectly simulate the preimage, and $\epsilon_{\mathsf{ps}} = 0$ holds. Let τ be a bound on the probability of I retrying the vinegar variables. MAYO's parameter sets ensure that $1 - q_{\mathsf{sign}}\tau > \frac{1}{2}$ holds, where the expected q_{sign} aligns with the security levels [10].

QR-UOV [29], PROV [26], and GeMSS [16] are provable secure since they follow the modified UOV/HFE signatures. If Rainbow [22] makes the same modification as the modified UOV signature, the scheme can be provably secure.

4.3 Extenstion to Security Proof of Fiat-Shamir with Aborts

The Fiat-Shamir with aborts paradigm [42] shares a similar structure with the probabilistic hash-and-sign with retry. Concurrent works by Devevey et al. [21]

and Barbosa et al. [3] demonstrate reductions of EUF-NMA ⇒ EUF-CMA for the Fiat-Shamir with aborts. Devevey et al. rely on the strong HVZK assumption [21, Definition 6], which allows for statistical simulation of protocol outputs even in cases of failure. Their proof uses the tight adaptive reprogramming technique to alter the signing oracle such that the EUF-NMA adversary can simulate using the statistical HVZK. In contrast, Barbosa et al. assume a weaker assumption called *accepting* HVZK assumption, which assumes that protocol outputs can be statistically simulated if the protocol does not fail [3, Definition 1]. This assumption closely aligns with the idea that a trapdoor function is *statistically* preimage-simulatable (see Definition 7). Essentially, their approach aligns with ours, involving the adaptive reprogramming followed by canceling the reprogramming during retries.

Given the structural similarity to the probabilistic hash-and-sign with retry, it is natural to explore the possibility of establishing a security proof for the Fiat-Shamir with aborts using the same techniques as presented in Theorem 1. In Appendix G, we present an alternative *tight* reduction of EUF-NMA ⇒ EUF-CMA for the Fiat-Shamir with aborts. The security bound, assuming the accepting HVZK, is almost identical to that of Barbosa et al. [3, Theorem 2].

5 Security Proof of Hash-and-Sign with Prefix Hashing in Multi-key Setting

In prefix hashing, the hash function H includes a small unpredictable portion of the verification key. Let $\mathsf{H}\colon \mathcal{U}\times\mathcal{R}\times\mathcal{M}\to\mathcal{Y}$ be a hash function and $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}]$ be a signature scheme adopting the probabilistic hash-and-sign with retry and prefix hashing, where $\mathsf{E}\colon \mathcal{Y}^{\mathcal{X}}\to\mathcal{U}$ is a deterministic function to extract a small unpredictable part of F into a key ID $u\in\mathcal{U}$. We assume that $\mathsf{E}(\mathsf{F})$ is uniform over $\mathcal{U}$ for $(\mathsf{F},\mathsf{I})\leftarrow\mathsf{Gen}(1^\lambda)$[11]. For a message m, $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}].\mathsf{Sign}$ repeats $r\leftarrow_{\$}\mathcal{R}$ and $x\leftarrow\mathsf{I}(\mathsf{H}(\mathsf{E}(\mathsf{F}),r,m))$ until $x\neq\bot$ holds, and outputs (r,x). For a verification key F, a message m, and a signature (r,x), $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T},\mathsf{H},\mathsf{E}].\mathsf{Vrfy}$ verifies by $\mathsf{F}(x)\overset{?}{=}\mathsf{H}(\mathsf{E}(\mathsf{F}),r,m)$.

We show that M-INV ⇒ M-EUF-CMA and M-CR ⇒ M-sEUF-CMA hold without any security loss in the number of keys q_{key} (see Lemma 8 in Appendix D and Lemma 9 in Appendix E). We note that there exist trivial reductions: $\mathrm{Adv}^{\text{M-INV}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{inv^m}})\leq q_{\mathsf{key}}\mathrm{Adv}^{\text{INV}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{inv}})$ and $\mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{cr^m}})\leq q_{\mathsf{key}}\mathrm{Adv}^{\text{CR}}_{\mathsf{T}}(\mathcal{B}_{\mathsf{cr}})$. To address this issue, we propose a generic method to show reductions from INV or CR by assuming the hardness of the computational problem on keys' distributions.

Let $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ be verification keys generated by Gen of a trapdoor fucntion T. Given a verification key $\mathsf{F}'\colon\mathcal{X}'\to\mathcal{Y}'$ generated by Gen' of another trapdoor function T', we simulate $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ by $\{\mathsf{L}_j\circ\mathsf{F}'\circ\mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$, where $\mathsf{L}_j\colon\mathcal{Y}'\to\mathcal{Y}$ and $\mathsf{R}_j\colon\mathcal{X}\to\mathcal{X}'$. Let $\mathcal{D}_{\mathsf{L}}$ and $\mathcal{D}_{\mathsf{R}}$ be some distributions of L_j and R_j. We note that

[11] If unpredictable parts do not exist or are computationally expensive to include in H, a fixed nonce can be used instead (the nonce is put in the verification key).

```
Game: $\mathsf{ST}_b$
$(\mathsf{F}', \mathsf{I}') \leftarrow \mathsf{Gen}'(1^\lambda)$
$b^* \leftarrow \mathcal{D}_{\mathsf{st}}^{\mathsf{NewKey}_b}()$
return $b^*$
```

```
$\mathsf{NewKey}_0()$
$(\mathsf{F}_j, \mathsf{I}_j) \leftarrow \mathsf{Gen}(1^\lambda)$
return $\mathsf{F}_j$
```

```
$\mathsf{NewKey}_1()$
$\mathsf{L}_j \leftarrow \mathcal{D}_{\mathsf{L}}$
$\mathsf{R}_j \leftarrow \mathcal{D}_{\mathsf{R}}$
$\mathsf{F}_j := \mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$
return $\mathsf{F}_j$
```

Fig. 12: ST (Sandwich Transformation) game

the domains and ranges of F' and F_j's may differ. We define a new game to give a bound on the distinguishing advantage of $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$ and $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$.

Definition 11 (ST (Sandwich Transformation) Game). *Let T and T' be trapdoor functions. Using a game given in Fig. 12, we define an advantage function of an adversary $\mathcal{D}_{\mathsf{st}}$ playing the* ST *game against T and T' as $\mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}}) = \left|\Pr\left[\mathsf{ST}_0^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right] - \Pr\left[\mathsf{ST}_1^{\mathcal{D}_{\mathsf{st}}} \Rightarrow 1\right]\right|$.*

We have the following reductions assuming some conditions on L_j and R_j (see the proofs in Appendices D and E.).

Lemma 6 (INV + ST ⇒ M-EUF-CMA). *Let T' be a trapdoor function with $\mathsf{F}' \colon \mathcal{X}' \to \mathcal{Y}$. Suppose that $\mathsf{L}_j \colon \mathcal{Y} \to \mathcal{Y}$ and $\mathsf{R}_j \colon \mathcal{X} \to \mathcal{X}'$ are used to simulate F_j by $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$ in the* ST *game, where L_j is a bijection.*

For any quantum M-EUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ of $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}, \mathsf{E}]$ with q_{key} keys and issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$, there exist an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of T', an* M-PS *adversary $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$ of $\mathsf{T}_{\mathsf{wpsf}}$ with q_{key} instances and issuing q_{sign} sampling queries, and an* ST *adversary $\mathcal{D}_{\mathsf{st}}$ of $(\mathsf{T}_{\mathsf{wpsf}}, \mathsf{T}')$ issuing q_{key} new key queries such that*

$$
\begin{aligned}
\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \leq{}& (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T}_{\mathsf{wpsf}}}(\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}) \\
&+ \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}}) + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} \\
&+ 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}} + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}, \qquad (11)
\end{aligned}
$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries and the running times of $\mathcal{B}_{\mathsf{inv}}$, $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$, and $\mathcal{D}_{\mathsf{st}}$ are about that of $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$.

Lemma 7 (CR + ST ⇒ M-sEUF-CMA). *Let T' be a trapdoor function with $\mathsf{F}' \colon \mathcal{X}' \to \mathcal{Y}$. Suppose that $\mathsf{L}_j \colon \mathcal{Y}' \to \mathcal{Y}$ and $\mathsf{R}_j \colon \mathcal{X} \to \mathcal{X}'$ are used to simulate F_j by $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$ in the* ST *game, where L_j and R_j are injections.*

For any quantum M-sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ of $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}}, \mathsf{H}, \mathsf{E}]$ with q_{key} keys and issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$, there exist a* CR *adversary*

$\mathcal{B}_{\mathsf{cr}}$ of T' and an ST *adversary $\mathcal{D}_{\mathsf{st}}$ of $(\mathsf{T}_{\mathsf{psf}}, \mathsf{T}')$ issuing q_{key} new key queries such that*

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}) \leq \frac{1}{1-2^{-\omega(\log(\lambda))}} \left(\mathrm{Adv}^{\mathrm{CR}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{cr}}) + \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{psf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})\right) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|},$$

where the running times of $\mathcal{B}_{\mathsf{cr}}$ and $\mathcal{D}_{\mathsf{st}}$ are about that of $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$.

In Appendix F, we apply the generic method to some frameworks of hash-and-sign signatures in lattice-based, code-based, and MQ-based cryptography. To bound the ST advantage, we introduce multi-instance variants of established computational problems in code-based and MQ-based cryptography, that is, permutation/linear equivalence [51] and morphism of polynomials [50].

Open problems: There are two open problems for the generic method. First, the computational problems used for bounding the ST advantage have not been studied deeply; therefore, future studies are necessary to guarantee the hardness of the problems. Second, we currently fail to use the generic method to show the M-EUF-CMA security under *adaptive corruptions of signing keys*. Solving this issue is the second open problem.

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva and Micciancio [13], pp. 269–295. https://doi.org/10.1007/978-3-030-26951-7_10 5, 12, 13, 14
2. Banegas, G., Carrier, K., Chailloux, A., Couvreur, A., Debris-Alazard, T., Gaborit, P., Karpman, P., Loyer, J., Niederhagen, R., Sendrier, N., et al.: Wave. Tech. rep., National Institute of Standards and Technology (2023), available at https://wave-sign.org/wave_documentation.pdf 6, 25, 35, 39
3. Barbosa, M., Barthe, G., Doczkal, C., Don, J., Fehr, S., Grégoire, B., Huang, Y.H., Hülsing, A., Lee, Y., Wu, X.: Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium. In: Handschuh and Lysyanskaya [33], pp. 358–389. https://doi.org/10.1007/978-3-031-38554-4_12 7, 26, 50, 53
4. Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: On the computational hardness of the code equivalence problem in cryptography. Advances in Mathematics of Communications **17**(1), 23–55 (Feb 2023). https://doi.org/10.3934/amc.2022064, /article/id/62fa202b4cedfd0007b8b288 48
5. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 93. pp. 62–73. ACM Press (Nov 1993). https://doi.org/10.1145/168588.168596 2, 9
6. Bellare, M., Rogaway, P.: The exact security of digital signatures: How to sign with RSA and Rabin. In: Maurer [43], pp. 399–416. https://doi.org/10.1007/3-540-68339-9_34 2, 5, 14
7. Belsley, E.D.: Rates of convergence of Markov chains related to association schemes. Harvard University (May 1993) 41

8. Beullens, W.: Not enough LESS: An improved algorithm for solving code equivalence problems over $\mathbb{F}_q$. In: Dunkelman, O., Jr., M.J.J., O'Flynn, C. (eds.) SAC 2020. LNCS, vol. 12804, pp. 387–403. Springer, Heidelberg (Oct 2020). https://doi.org/10.1007/978-3-030-81652-0_15 48
9. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 348–373. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_13 42
10. Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.: MAYO. Tech. rep., National Institute of Standards and Technology (2023), available at https://pqmayo.org/assets/specs/mayo.pdf 6, 25, 35, 38, 42, 43
11. Beullens, W., Chen, M.S., Ding, J., Gong, B., Kannwischer, M.J., Patarin, J., Peng, B.Y., Schmidt, D., Shih, Cheng-Jhih Tao, C., Yang, B.Y.: UOV. Tech. rep., National Institute of Standards and Technology (2023), available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/UOV-spec-web.pdf 36, 40
12. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part II. LNCS, vol. 11892, pp. 61–90. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-36033-7_3 13
13. Boldyreva, A., Micciancio, D. (eds.): CRYPTO 2019, Part II, LNCS, vol. 11693. Springer, Heidelberg (Aug 2019) 28, 30
14. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (Dec 2011). https://doi.org/10.1007/978-3-642-25385-0_3 3, 5, 15, 16, 17, 46
15. Bouillaguet, C., Fouque, P.A., Véber, A.: Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 211–227. Springer, Heidelberg (May 2013). https://doi.org/10.1007/978-3-642-38348-9_13 49
16. Casanova, A., Faugère, J.C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: GeMSS. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions 6, 25, 38
17. Chailloux, A., Debris-Alazard, T.: Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 453–479. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45388-6_16 3, 4, 5, 9, 15, 16, 17, 23, 25, 35, 40
18. Chatterjee, S., Das, M.P.L., Pandit, T.: Revisiting the security of salted UOV signature. In: Isobe, T., Sarkar, S. (eds.) Progress in Cryptology – INDOCRYPT 2022. LNCS, vol. 13774, pp. 697–719. Springer, Heidelberg (Jan 2022) 2, 17
19. Courtois, N., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 157–174. Springer, Heidelberg (Dec 2001). https://doi.org/10.1007/3-540-45682-1_10 2, 39
20. Dallot, L.: Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme. In: WEWoRC 2007. LNCS, vol. 4945, pp. 65–77. Springer, Heidelberg (Jul 2007) 6, 25, 34, 39

21. Devevey, J., Fallahpour, P., Passelègue, A., Stehlé, D.: A detailed analysis of fiat-shamir with aborts. In: Handschuh and Lysyanskaya [33], pp. 327–357. https://doi.org/10.1007/978-3-031-38554-4_11 7, 25, 26
22. Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D., Yang, B.Y., Kannwischer, M.J., Patarin, J.: Rainbow. Tech. rep., National Institute of Standards and Technology (2020), available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions 6, 25, 37
23. Don, J., Fehr, S., Majenz, C.: The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part III. LNCS, vol. 12172, pp. 602–631. Springer, Heidelberg (Aug 2020). https://doi.org/10.1007/978-3-030-56877-1_21 6, 12, 13, 17
24. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Security of the Fiat-Shamir transformation in the quantum random-oracle model. In: Boldyreva and Micciancio [13], pp. 356–383. https://doi.org/10.1007/978-3-030-26951-7_13 24
25. Duman, J., Hövelmanns, K., Kiltz, E., Lyubashevsky, V., Seiler, G.: Faster lattice-based KEMs via a generic fujisaki-okamoto transform using prefix hashing. In: Vigna, G., Shi, E. (eds.) ACM CCS 2021. pp. 2722–2737. ACM Press (Nov 2021). https://doi.org/10.1145/3460120.3484819 4
26. Faugere, J.C., Fouque, P.A., Macario-Rat, G., Minaud, B., Patarin, J.: PROV. Tech. rep., National Institute of Standards and Technology (2023), available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/prov-spec-web.pdf 6, 25, 37
27. Faugère, J.C., Perret, L.: Polynomial equivalence problems: Algorithmic and theoretical aspects. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 30–47. Springer, Heidelberg (May / Jun 2006). https://doi.org/10.1007/11761679_3 49
28. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO'86. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (Aug 1987). https://doi.org/10.1007/3-540-47721-7_12 2
29. Furue, H., Ikematsu, Y., Hoshino, F., Kiyomura, Y., Saito, T., Takagi, T.: QR-UOV. Tech. rep., National Institute of Standards and Technology (2023), available at http://info.isl.ntt.co.jp/crypt/qruov/files/NISTPQC_QRUOV.pdf 6, 25, 37
30. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/1374376.1374407 2, 5, 9, 14, 43, 47, 48
31. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. **17**(2), 281–308 (1988). https://doi.org/10.1137/0217017, https://doi.org/10.1137/0217017 2
32. Grilo, A.B., Hövelmanns, K., Hülsing, A., Majenz, C.: Tight adaptive reprogramming in the QROM. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 637–667. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92062-3_22 3, 5, 7, 12, 24, 33
33. Handschuh, H., Lysyanskaya, A. (eds.): CRYPTO 2023, Part V, LNCS, vol. 14085. Springer, Heidelberg (Aug 2023) 28, 30
34. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 275–304. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_10 2, 9

35. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (Mar 2016). https://doi.org/10.1007/978-3-662-49384-7_15 12
36. Ikematsu, Y., Nakamura, S., Santoso, B., Yasuda, T.: Security analysis on an ElGamal-like multivariate encryption scheme based on isomorphism of polynomials. In: Yu, Y., Yung, M. (eds.) Information Security and Cryptology – Inscrypt 2021. LNCS, vol. 13007, pp. 235–250. Springer, Heidelberg (Oct 2021) 49
37. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 552–586. Springer, Heidelberg (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_18 7
38. Kiltz, E., Masny, D., Pan, J.: Optimal security proofs for signatures from identification schemes. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 33–61. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53008-5_2 10
39. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT'99. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (May 1999). https://doi.org/10.1007/3-540-48910-X_15 2, 25, 35, 40
40. Leon, J.: Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory **28**(3), 496–511 (May 1982), https://ieeexplore.ieee.org/document/1056498 48
41. Liu, Y., Jiang, H., Zhao, Y.: Tighter post-quantum proof for plain FDH, PFDH and GPV-IBE. Cryptology ePrint Archive, Report 2022/1441 (2022), https://eprint.iacr.org/2022/1441 6, 7, 15, 17, 32
42. Lyubashevsky, V.: Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (Dec 2009). https://doi.org/10.1007/978-3-642-10366-7_35 7, 25
43. Maurer, U.M. (ed.): EUROCRYPT'96, LNCS, vol. 1070. Springer, Heidelberg (May 1996) 28, 31
44. Menezes, A., Smart, N.: Security of signature schemes in a multi-user setting. Designs, Codes and Cryptography **33**(3), 261–274 (Nov 2004), https://link.springer.com/article/10.1023/B:DESI.0000036250.18062.3f 4
45. Morozov, K., Roy, P.S., Steinwandt, R., Xu, R.: On the security of the Courtois-Finiasz-Sendrier signature. Open Mathematics **16**(1), 161–167 (Mar 2018). https://doi.org/doi:10.1515/math-2018-0011, https://doi.org/10.1515/math-2018-0011 34
46. NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (Jan 2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf 4
47. NIST: Call for additional digital signature schemes for the post-quantum cryptography standardization process (Sep 2022), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf 3, 6
48. NIST: Status report on the third round of the nist post-quantum cryptography standardization process (Sep 2022), https://csrc.nist.gov/publications/detail/nistir/8413/final 3
49. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer [43], pp. 33–48. https://doi.org/10.1007/3-540-68339-9_4 2, 35

50. Patarin, J., Goubin, L., Courtois, N.: Improved algorithms for isomorphisms of polynomials. In: Nyberg, K. (ed.) EUROCRYPT'98. LNCS, vol. 1403, pp. 184–200. Springer, Heidelberg (May / Jun 1998). https://doi.org/10.1007/BFb0054126 28, 49
51. Petrank, E., Roth, R.M.: Is code equivalence easy to decide? IEEE Transactions on Information Theory **43**(5), 1602–1604 (Sep 1997), https://ieeexplore.ieee.org/document/623157 28, 48
52. Prest, T., Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 47
53. Sakumoto, K., Shirai, T., Hiwatari, H.: On provable security of UOV and HFE signature schemes against chosen-message attack. In: Yang, B.Y. (ed.) Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011. pp. 68–82. Springer, Heidelberg (Nov / Dec 2011). https://doi.org/10.1007/978-3-642-25405-5_5 2, 4, 5, 6, 9, 14, 15, 25, 36, 37, 38, 40, 41
54. Sendrier, N.: Finding the permutation between equivalent linear codes: The support splitting algorithm. IEEE Transactions on Information Theory **46**(4), 1193–1203 (2000) 48
55. Sendrier, N., Simos, D.E.: The hardness of code equivalence over and its application to code-based cryptography. In: Gaborit, P. (ed.) Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013. pp. 203–216. Springer, Heidelberg (Jun 2013). https://doi.org/10.1007/978-3-642-38616-9_14 48
56. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th FOCS. pp. 124–134. IEEE Computer Society Press (Nov 1994). https://doi.org/10.1109/SFCS.1994.365700 2
57. Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced Oil and Vinegar. In: Paterson, K.G., Stebila, D. (eds.) SAC 2019. LNCS, vol. 11959, pp. 574–588. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-38471-5_23 49
58. Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part II. LNCS, vol. 8617, pp. 1–18. Springer, Heidelberg (Aug 2014). https://doi.org/10.1007/978-3-662-44381-1_1 12
59. Yamakawa, T., Zhandry, M.: Classical vs quantum random oracles. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part II. LNCS, vol. 12697, pp. 568–597. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77886-6_20 3, 4, 5, 15, 16, 23
60. Yamakawa, T., Zhandry, M.: Verifiable quantum advantage without structure. In: 63rd FOCS. pp. 69–74. IEEE Computer Society Press (Oct / Nov 2022). https://doi.org/10.1109/FOCS54457.2022.00014 3
61. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. Cryptology ePrint Archive, Report 2012/076 (2012), https://eprint.iacr.org/2012/076 3, 4, 5, 15, 16, 17, 23

A Issue with Security Proof of [41]

We have identified a flaw in the proof of OW ⇒ EUF-CMA presented in Theorem 2 of the latest version published on January 28, 2023 [41]. Let $\mathsf{HaS}[\mathsf{T}_{\mathsf{tdp}}, \mathsf{H}]$ be a signature scheme adopting the deterministic hash-and-sign, where $\mathsf{T}_{\mathsf{tdp}}$ is a trapdoor permutation and $\mathsf{H} \in \mathcal{Y}^{\mathcal{M}}$. In the security proof, the random function H is replaced by $\mathsf{H} = \mathsf{F}(\widetilde{\mathsf{H}}(m))$, where $\widetilde{\mathsf{H}} \leftarrow_{\$} \mathcal{X}^{\mathcal{M}}$, and the signing oracle returns $\widetilde{\mathsf{H}}(m)$. The security proof relies on the measure-and-reprogram technique [32] and involves a two-stage algorithm S composed of S_1 and S_2, which interacts with $\mathcal{A}_{\mathsf{cma}}$ in the modified EUF-CMA game. The algorithm S behaves as follows:

1. Choose $(i, b) \leftarrow_{\$} ([q] \times \{0, 1\}) \cup \{(q + 1, 0)\}$.
2. Run $\mathcal{A}_{\mathsf{cma}}$ with $\widetilde{\mathsf{H}}$ until i-th query.
3. Measure i-th query and output m as the output of S_1.
4. Given a random θ, reprogram $\widetilde{\mathsf{H}}' = \widetilde{\mathsf{H}}^{m \mapsto \theta}$.
5. If $i = q + 1$, then go to Step 8.
6. Answer i-th query with $\widetilde{\mathsf{H}}$ (if $b = 0$) or $\widetilde{\mathsf{H}}'$ (if $b = 1$).
7. Run $\mathcal{A}_{\mathsf{cma}}$ with $\widetilde{\mathsf{H}}'$ until the end.
8. Output $\mathcal{A}_{\mathsf{cma}}$'s output (m^*, x^*) as the output of S_2.

The authors argue that the following inequality holds from Lemma 2.

$$\begin{aligned}\Pr\Big[x = \theta : m \leftarrow \mathsf{S}_1^{\mathcal{A}_{\mathsf{cma}}}(), (m, x) \leftarrow \mathsf{S}_2^{\mathcal{A}_{\mathsf{cma}}}(\theta)\Big] \\ \geq \frac{1}{(2q+1)^2} \Pr\Big[x = \widetilde{\mathsf{H}}(m) : (m, x) \leftarrow \mathcal{A}_{\mathsf{cma}}^{|\mathsf{H}\rangle}(\mathsf{F})\Big] . \quad (12)\end{aligned}$$

In the original version published on October 22, 2022, the index i is chosen from all the queries to $\widetilde{\mathsf{H}}$ ($q = q_{\mathsf{qro}} + q_{\mathsf{sign}}$), while in the latest version, it is chosen only from queries to $\widetilde{\mathsf{H}}$ outside the signing oracle ($q = q_{\mathsf{qro}}$). The latter implies that, within the signing oracle, query inputs for $\widetilde{\mathsf{H}}$ are not measured and $\widetilde{\mathsf{H}}$ is not reprogrammed.

If we carefully examine the proof of the measure-and-reprogram technique [32, Theorem 2], we find issues with the latest version's approach. In the proof, the measure-and-reprogram technique relies on the assumption that when applying $\mathbb{1} - |m\rangle\langle m|$ (where $\mathbb{1}$ is the identity operator) onto the query input register at the i-th query, the quantum states in the following two cases are identical:

- Answers the i-th query by $\widetilde{\mathsf{H}}$ and responds to subsequent queries by $\widetilde{\mathsf{H}}'$.
- Answers the i-th query by $\widetilde{\mathsf{H}}'$ and responds to subsequent queries by $\widetilde{\mathsf{H}}'$.

If i indicates the index of queries to $\widetilde{\mathsf{H}}$ outside the signing oracle, either $\widetilde{\mathsf{H}}$ (in the first case) or $\widetilde{\mathsf{H}}'$ (in the second case) is queried in the signing oracle between the i-th and $(i+1)$-th queries. Due to this difference in the signing oracle's behavior, the quantum states are not necessarily identical. The authors claim that queries to $\widetilde{\mathsf{H}}$ within the signing oracle can be disregarded based on the observation that when $\mathcal{A}_{\mathsf{cma}}$ does not output 0, it implies that the observed m has not been queried for the signing oracle. However, they need to clearly demonstrate how this fact affects the above assumption and Eq. (12).

B Security Proofs of Hash-and-sign Signatures by Theorem 1 and Corollary 1

This section shows the applications of Theorem 1 and Corollary 1 to some code-based and MQ-based hash-and-sign signatures.

B.1 Code-based Cryptography

Application to the Modified CSF Signature: Dallot [20] proposed a modification to the CFS signature, that is, the adaption of the probabilistic hash-and-sign with retry. For the details of the (modified) CFS signature, see Appendix C.1. Let $\mathsf{T}_{\mathsf{cfs}} = (\mathsf{Gen}_{\mathsf{cfs}}, \mathsf{F}_{\mathsf{cfs}}, \mathsf{I}_{\mathsf{cfs}})$ be the underlying trapdoor function of the modified CFS signature and $\mathcal{X}_{n,\leq t} = \{x \in \mathbb{F}_2^n : 0 < \mathsf{hw}(x) \leq t\}$ be a domain of $\mathsf{F}_{\mathsf{cfs}}$, where $\mathsf{hw}(x)$ denotes a Hamming weight of x. $\mathsf{F}_{\mathsf{cfs}} = UH_0P$ ($\mathsf{F}_{\mathsf{cfs}} : \mathcal{X}_{n,\leq t} \to \mathbb{F}_2^{n-k}$) consists of a parity-check matrix of an (n,k)-binary Goppa code $H_0 \in \mathbb{F}_2^{(n-k)\times n}$, an invertible matrix $U \in \mathbb{F}_2^{(n-k)\times(n-k)}$, and a permutation matrix $P \in \mathbb{F}_2^{n\times n}$. Since we assume that the (n,k)-binary Goppa code can decode up to t errors, one-to-one correspondence exists between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec} = \{y \in \mathbb{F}_2^{n-k} : y(U^{-1})^T \text{ is decodable}\}$. Therefore, $\mathsf{F}_{\mathsf{cfs}} : \mathcal{X}_{n,\leq t} \to \mathbb{F}_2^{n-k}$ is an injection. Using the fact, Morozov et al. gave a reduction of INV ⇒ sEUF-CMA in the ROM [45, Theorem 3.1]. We show that the modified CFS signature is sEUF-CMA-secure in the QROM, assuming that $\mathsf{T}_{\mathsf{cfs}}$ is non-invertible.

Proposition 1 (INV ⇒ sEUF-CMA (Modified CFS Signature)). *For any quantum* sEUF-CMA *adversary $\mathcal{A}_{\mathsf{cma}}$ of $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}]$ issuing at most q_{sign} classical queries to the signing oracle and q_{qro} (quantum) random oracle queries to $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$, there exists an* INV *adversary $\mathcal{B}_{\mathsf{inv}}$ of $\mathsf{T}_{\mathsf{cfs}}$ such that*

$$\mathrm{Adv}^{\text{sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{cfs}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries and the running time of $\mathcal{B}_{\mathsf{inv}}$ is about that of $\mathcal{A}_{\mathsf{cma}}$.

Proof. When we define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ as $x \leftarrow_\$ \mathcal{X}_{n,\leq t}$, $\mathsf{T}_{\mathsf{cfs}}$ becomes WPSF. Since $\mathsf{F}_{\mathsf{cfs}}$ is an injection, we can apply Corollary 1 to the modified CFS signature. In the PS game, we show that $\mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ in Sample_1 can perfectly simulate x_i output by Sample_0. From the one-to-one correspondence between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec}$, $x \leftarrow \mathsf{I}_{\mathsf{cfs}}(y)$ for $y \leftarrow_\$ \mathcal{Y}_{dec}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$. Also, Sample_0 outputs x_i after retrying $y_i \leftarrow_\$ \mathbb{F}_2^{n-k}$ until $\mathsf{I}_{\mathsf{cfs}}(y_i) \neq \bot$ holds; therefore y_i is uniformly chosen from $\mathcal{Y}_{dec}$. Hence, the distribution of x_i output by Sample_0 is equivalent to that of $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{cfs}})$ and, thus, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{cfs}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

Application to Wave: Wave is a practical and unbroken hash-and-sign signature [2]. See Appendix C.2 for the details. Wave adopts the probabilistic hash-and-sign (without retry) and Wave's trapdoor function $\mathsf{T}_{\mathsf{wave}} = (\mathsf{Gen}_{\mathsf{wave}}, \mathsf{F}_{\mathsf{wave}}, \mathsf{I}_{\mathsf{wave}})$ is ATPSF [17] (see Section 4.2). We show that Wave is EUF-CMA-secure using one of the conditions of ATPSF.

Proposition 2 (INV ⇒ EUF-CMA (Wave)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{wave}}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exists an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{wave}}$ *such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{wave}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{wave}}}(\mathcal{B}_{\mathsf{inv}}) + q_{\mathsf{sign}}\delta + \frac{3}{2} q_{\mathsf{sign}} \sqrt{\frac{q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}},$$

where the running time of $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Since $\mathsf{T}_{\mathsf{wave}}$ is ATPSF [17] that is a special case of WPSF, we can apply Theorem 1 to Wave. From the first condition of ATPSF, there is a bound δ on the expectation of $\delta_{\mathsf{F},\mathsf{I}} = \Delta(\mathsf{SampDom}(\mathsf{F}_{\mathsf{wave}}), \mathsf{I}_{\mathsf{wave}}(\mathsf{U}(\mathcal{Y})))$; therefore, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{wave}}}(\mathcal{D}_{\mathsf{ps}}) \leq q_{\mathsf{sign}}\delta$ holds from the union bound. □

Compared with the existing reduction using Eq. (1) [17], the factor of δ is not a square root in our reduction. Also, its security can be proved on the basis of hardness assumption of the syndrome decoding since there is a tight reduction from the syndrome decoding to the INV of $\mathsf{T}_{\mathsf{wave}}$ [17, Proposition 8].

B.2 Multivariate-quadratic-based Cryptography

Many schemes based on the UOV [39] and HFE [49] signatures have been proposed. Sakumoto et al. proposed modifications of the schemes adopting the probabilistic hash-and-sign with retry. We prove that the original/modified UOV signatures and the modified HFE signature are EUF-CMA-secure in the QROM if their trapdoor functions are non-invertible. Also, we prove the EUF-CMA security of MAYO [10].

Application to the Original UOV Signature: We briefly review the Original UOV scheme. For the details, see Appendix C.3. Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ be a trapdoor function used in the original UOV signature. $\mathsf{F}_{\mathsf{uov}} = \mathsf{P} \circ \mathsf{S}$ ($\mathsf{F}_{\mathsf{uov}} \colon \mathbb{F}_q^n \to \mathbb{F}_q^o$) consists of a multivariate quadratic map $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$ and an invertible affine map $\mathsf{S} \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$. Variables in P are called vinegar variables $z^v \in \mathbb{F}_q^v$ and oil variables $z^o \in \mathbb{F}_q^o$, where $n = v+o$. By design of P, $\mathsf{P}(z^v, \cdot)$ becomes a set of linear functions on oil variables z^o by fixing z^v. $\mathsf{I}_{\mathsf{uov}}$ chooses $z^v \leftarrow_{\$} \mathbb{F}_q^v$ and obtains z^o after retrying z^v until $\{z^o : \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$ holds (or $\mathsf{P}(z^v, z^o)$ has full-rank). See Fig. 13 for the signing algorithm and $\mathsf{I}_{\mathsf{uov}}$.

We show the EUF-CMA security of the original UOV signature in the QROM if it adopts the probabilistic hash-and-sign.

```
$\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}_{\mathsf{uov}}, m)$
  $r \leftarrow_\$ \mathcal{R}$
  $x \leftarrow \mathsf{I}_{\mathsf{uov}}(\mathsf{H}(r, m))$
  return $(r, x)$

$\mathsf{I}_{\mathsf{uov}}(y)$
  repeat
      $z^v \leftarrow_\$ \mathbb{F}_q^v$
  until $\{z^o : \mathsf{P}(z^v, z^o) = y\} \neq \emptyset$
  $z^o \leftarrow_\$ \{z^o : \mathsf{P}(z^v, z^o) = y\}$
  $x := \mathsf{S}^{-1}(z^v \| z^o)$
  return $x$
```

Fig. 13: Signature generation algorithm of the original UOV signature

Proposition 3 (INV ⇒ EUF-CMA (Original UOV Signature)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R} \times \mathcal{M}}$*, there exist an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{uov}}$ *and a* PS *adversary* $\mathcal{D}_{\mathsf{ps}}$ *of* $\mathsf{T}_{\mathsf{uov}}$ *issuing* q_{sign} *sampling queries such that*

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{uov}}, \mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}} + 1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{D}_{\mathsf{ps}}) + \frac{3}{2} q_{\mathsf{sign}} \sqrt{\frac{q_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}},$$

where the running times of $\mathcal{B}_{\mathsf{inv}}$ *and* $\mathcal{D}_{\mathsf{ps}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Defining $\mathsf{SampDom}(\mathsf{F}_{\mathsf{uov}})$ as $x \leftarrow_\$ \mathbb{F}_q^n$, $\mathsf{T}_{\mathsf{uov}}$ becomes WPSF; therefore, we can apply Theorem 1. □

If $\mathsf{T}_{\mathsf{uov}}$ is preimage-simulatable ($\mathrm{Adv}^{\mathrm{PS}}_{\mathsf{T}_{\mathsf{uov}}}(\mathcal{D}_{\mathsf{ps}})$ is negligible), the original UOV signature is provable secure. However, we must consider the *computational* indistinguishability of $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ ($b = 0$) and $x \leftarrow_\$ \mathbb{F}_q^n$ ($b = 1$) in the PS game since the former x is not uniform. Note that we can apply Proposition 3 to the UOV signature scheme recently submitted to the NIST PQC standardization [11][12].

Application to the Modified UOV Signature: Sakumoto et al. [53] proposed the modified UOV signature to solve the problem of the original one, that is, the non-uniformity of $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$. For the details, see Appendix C.3. Let $\mathsf{T}_{\mathsf{muov}} = (\mathsf{Gen}_{\mathsf{muov}}, \mathsf{F}_{\mathsf{muov}}, \mathsf{I}_{\mathsf{muov}})$ be a trapdoor function used in the modified UOV signature ($\mathsf{Gen}_{\mathsf{muov}} = \mathsf{Gen}_{\mathsf{uov}}$ and $\mathsf{F}_{\mathsf{muov}} = \mathsf{F}_{\mathsf{uov}}$) and Fig. 14 depicts $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}$ and $\mathsf{I}_{\mathsf{muov}}$. The modified UOV signature retries r instead of z^v and $\mathsf{I}_{\mathsf{muov}}$ is divided into two functions; $\mathsf{I}^1_{\mathsf{muov}}$ and $\mathsf{I}^2_{\mathsf{muov}}$. $\mathsf{I}^1_{\mathsf{muov}}$ chooses $z^v \leftarrow_\$ \mathbb{F}_q^v$ and $\mathsf{I}^2_{\mathsf{muov}}$ finds z^o after retrying r until $\{z^o : \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$ holds. Considering the difference in the signing procedure, we show the EUF-CMA security of the modified UOV signature in the QROM.

[12] The UOV signature scheme [11] retries the vinegar variable z^v until $\mathsf{P}(z^v, \cdot)$ becomes full rank. As a consequence of retrying z^v, z^v is not uniform.

```
$\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}(\mathsf{I}_{\mathsf{muov}}, m)$
  $z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$
  repeat
      $r \leftarrow_\$ \mathcal{R}$
      $x \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, \mathsf{H}(r, m))$
  until $x \neq \bot$
  return $(r, x)$

$\mathsf{I}^1_{\mathsf{muov}}()$
  $z^v \leftarrow_\$ \mathbb{F}_q^v$
  return $z^v$

$\mathsf{I}^2_{\mathsf{muov}}(z^v, y)$
  if $\{z^o : \mathsf{P}(z^v, z^o) = y\} = \emptyset$ then
      return $\bot$
  $z^o \leftarrow_\$ \{z^o : \mathsf{P}(z^v, z^o) = y\}$
  $x := \mathsf{S}^{-1}(z^v \| z^o)$
  return $x$
```

Fig. 14: Signature generation algorithm of the modified UOV signature

Proposition 4 (INV ⇒ EUF-CMA (Modified UOV Signature)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exists an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{muov}}$ *such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{muov}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries and the running time of* $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Defining $\mathsf{SampDom}(\mathsf{F}_{\mathsf{muov}})$ as $x \leftarrow_\$ \mathbb{F}_q^n$, $\mathsf{T}_{\mathsf{muov}}$ becomes WPSF. Considering the signing procedure of the modified UOV signature, we modify the signing oracles of G_0-G_4 in the proof of Theorem 1 and Sample_0 of the PS game by adding $z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$ in the beginning and replacing $x_i \leftarrow \mathsf{I}(y_i)$ with $x_i \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, y_i)$. Then, $\mathcal{D}_{\mathsf{ps}}$ playing the modified PS game can simulate G_4 $(b = 0)$ and G_5 $(b = 1)$. Hence, we can apply Theorem 1 to the modified UOV signature. In Sample_0 of the PS game, $x_i \leftarrow \mathsf{I}^2_{\mathsf{muov}}(z^v, y)$ for $z^v \leftarrow \mathsf{I}^1_{\mathsf{muov}}()$ after retrying y follows $\mathsf{U}(\mathbb{F}_q^n)$ form [53, Theorem 1] (we show the proof sketch in Appendix C.3); therefore, $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{muov}})$ in Sample_1 is indistinguishable form x_i output by Sample_0. Hence, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{muov}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

We can apply Proposition 4 to QR-UOV [29] and PROV [26] without modification. For Rainbow [22], it requires the same modification as the modified UOV signature.

Application to the Modified HFE Signature: The modified HFE signature proposed by Sakumoto et al. [53] is designed for the same purpose as the modified UOV signature. For the details, see Appendix C.4. Let $\mathsf{T}_{\mathsf{mhfe}} = (\mathsf{Gen}_{\mathsf{mhfe}}, \mathsf{F}_{\mathsf{mhfe}}, \mathsf{I}_{\mathsf{mhfe}})$ be a trapdoor function used in the modified HFE scheme. We show that the modified HFE signature is EUF-CMA secure.

Proposition 5 (INV ⇒ EUF-CMA (Modified HFE Signature)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}]$ *issuing at most* q_{sign}

classical queries to the signing oracle and q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exists an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{mhfe}}$ *such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq (2q_{\mathsf{qro}}+1)^2\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{mhfe}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}},$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries and the running time of* $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. Since $\mathsf{F}_{\mathsf{mhfe}}$ has a domain $\mathbb{F}_q^n$, we can define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{mhfe}})$ as $x \leftarrow_{\$} \mathbb{F}_q^n$. Then, $\mathsf{T}_{\mathsf{mhfe}}$ becomes WPSF and we can apply Theorem 1 to the modified HFE scheme. The authors of [53] showed that $x \leftarrow \mathsf{I}_{\mathsf{mhfe}}(y)$ after retrying y is uniformly distributed over $\mathbb{F}_q^n$ (we show the proof sketch in Appendix C.4). Therefore, in the PS game, $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_{\mathsf{mhfe}})$ in Sample_1 is indistingushable from x_i output by Sample_0, and thus, $\mathrm{Adv}^{\text{PS}}_{\mathsf{T}_{\mathsf{mhfe}}}(\mathcal{D}_{\mathsf{ps}}) = 0$ holds. □

We can apply Proposition 5 to GeMSS [16].

Application to MAYO: MAYO, proposed by Beullens [10], is a signature scheme that adopts the probabilistic hash-and-sign and its trapdoor function is based on UOV. For the details, see Appendix C.5. Let $\mathsf{T}_{\mathsf{mayo}} = (\mathsf{Gen}_{\mathsf{mayo}}, \mathsf{F}_{\mathsf{mayo}}, \mathsf{I}_{\mathsf{mayo}})$ be a trapdoor function used in MAYO. $\mathsf{I}_{\mathsf{mayo}}$ finds a preimage $x = x^v + x^o$ of y for a multivariate quadratic map $\mathsf{P}^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$. Once x^v is uniformly chosen from $(\mathbb{F}_q^{n-o}\times\{0^o\})^k \subset \mathbb{F}_q^{kn}$, where 0^o denotes a vector of o 0s, $\mathsf{P}^*(x^v+x^o) = y$ becomes a linear system of equations for x^o. $\mathsf{I}_{\mathsf{mayo}}$ outputs a preimage after retrying x^v until $\mathsf{P}^*(x^v+x^o)$ has full rank. If $\mathsf{I}_{\mathsf{mayo}}$ outputs x without needing to retry x^v, x is uniformly distributed over $\mathbb{F}_q^{kn}$. Let τ be a bound on the probability that $\mathsf{P}^*(x^v+x^o)$ does not have full rank for a random x^v. MAYO is EUF-CMA-secure in the ROM [10, Theorem 1] assuming that $q_{\mathsf{sign}}\tau < \frac{1}{2}$. Under the same assumption, we show the EUF-CMA security of MAYO in the QROM.

Proposition 6 (INV⇒EUF-CMA (MAYO)). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{Y}^{\mathcal{R}\times\mathcal{M}}$*, there exists an* INV *adversary* $\mathcal{B}_{\mathsf{inv}}$ *of* $\mathsf{T}_{\mathsf{mayo}}$ *such that*

$$\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{(2q_{\mathsf{qro}}+1)^2}{1-q_{\mathsf{sign}}\tau}\mathrm{Adv}^{\text{INV}}_{\mathsf{T}_{\mathsf{mayo}}}(\mathcal{B}_{\mathsf{inv}}) + \frac{3}{2}q_{\mathsf{sign}}\sqrt{\frac{q_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}},$$

where the running time of $\mathcal{B}_{\mathsf{inv}}$ *is about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. We apply Theorem 1 with defining an intermediate game G'_1. G'_1 is identical to G_1 except that G'_1 aborts and outputs 0 whenever $\mathsf{I}_{\mathsf{mayo}}$ retries x^v. The probability that G'_1 does not abort while q_{sign} signing queries is at least

$1 - q_{\mathsf{sign}}\tau$. Therefore, $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \frac{1}{1-q_{\mathsf{sign}}\tau} \Pr\left[\mathsf{G}_1'^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. We define $\mathsf{SampDom}(\mathsf{F}_{\mathsf{mayo}})$ as $x \leftarrow_\$ \mathbb{F}_q^{kn}$. The adversary of G_5 perfectly simulates the signing oracle in the case that G_1' does not abort by using his oracle since $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ follows $\mathsf{U}(\mathbb{F}_q^{kn})$. Therefore, the view of the adversary is identical in the simulated one with the case that G_1' does not abort, and thus $\Pr\left[\mathsf{G}_1'^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ holds. Since the EUF-NMA adversary can simulate G_5, $\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{mayo}},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}})$ holds, which yields the claimed bound. □

C Review of Hash-and-sign Signatures

C.1 Modified CFS Signature [20]

The modified CFS signature adopts the probabilistic hash-and-sign with retry. Let $\mathsf{T}_{\mathsf{cfs}} = (\mathsf{Gen}_{\mathsf{cfs}}, \mathsf{F}_{\mathsf{cfs}}, \mathsf{I}_{\mathsf{cfs}})$ be a trapdoor function used in the modified CFS signature. We assume that an (n,k)-binary Goppa code can decode up to t errors. $\mathsf{Gen}_{\mathsf{cfs}}$ generates a parity-check matrix $H_0 \in \mathbb{F}_2^{(n-k)\times n}$ of the (n,k)-binary Goppa code, an invertible matrix $U \in \mathbb{F}_2^{(n-k)\times(n-k)}$, and a permutation matrix $P \in \mathbb{F}_2^{n\times n}$, and outputs $H = UH_0P \in \mathbb{F}_2^{(n-k)\times n}$ as $\mathsf{F}_{\mathsf{cfs}}$ and (U, H_0, P) as $\mathsf{I}_{\mathsf{cfs}}$. On input $x \in \mathcal{X}_{n,\leq t} = \{x \in \mathbb{F}_2^n : 0 < \mathsf{hw}(x) \leq t\}$, the function $\mathsf{F}_{\mathsf{cfs}}$ computes a syndrome $y := xH^T \in \mathbb{F}_2^{n-k}$. On input $y \in \mathbb{F}_2^{n-k}$, the trapdoor $\mathsf{I}_{\mathsf{cfs}}$ composed of (U, H_0, P) computes an error vector as follows: It decodes $y(U^{-1})^T$ using H_0 to obtain x', and outputs an error vector $x = x'(P^{-1})^T$; if $y(U^{-1})^T$ is not decodable, it outputs $\perp$. Since the (n,k)-binary Goppa code can decode up to t errors, which is our assumption, there is a one-to-one correspondence between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec} = \{y \in \mathbb{F}_2^{n-k} : y(U^{-1})^T \text{ is decodable}\}$. Therefore, $\mathsf{F}_{\mathsf{cfs}}$ is injective and $\mathsf{I}_{\mathsf{cfs}}(y)$ outputs a preimage for $y \leftarrow_\$ \mathbb{F}_2^{n-k}$ with probability $\frac{|\mathcal{Y}_{dec}|}{|\mathbb{F}_2^{n-k}|} = \frac{|\mathcal{X}_{n,\leq t}|}{|\mathbb{F}_2^{n-k}|}$. As shown in [19], $\frac{|\mathcal{X}_{n,\leq t}|}{|\mathbb{F}_2^{n-k}|} \approx \frac{1}{t!}$ holds and we can take $q'_{\mathsf{sign}} = ct!q_{\mathsf{sign}}$ for some constant $c > 1$ in Proposition 1.

We show that a preimage x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$. Initially, $x \leftarrow \mathsf{I}_{\mathsf{cfs}}(y)$ for $y \leftarrow_\$ \mathcal{Y}_{dec}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$ from the one-to-one correspondence between $\mathcal{X}_{n,\leq t}$ and $\mathcal{Y}_{dec}$. Subsequently, $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ outputs x after retrying $y \leftarrow_\$ \mathbb{F}_2^{n-k}$ until $\mathsf{I}_{\mathsf{cfs}}(y) \neq \perp$ holds; therefore the chosen y follows $\mathsf{U}(\mathcal{Y}_{dec})$. Hence, x output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{cfs}}, \mathsf{H}].\mathsf{Sign}$ follows $\mathsf{U}(\mathcal{X}_{n,\leq t})$.

C.2 Wave [2]

Wave adopts the probabilistic hash-and-sign. Let $\mathsf{T}_{\mathsf{wave}} = (\mathsf{Gen}_{\mathsf{wave}}, \mathsf{F}_{\mathsf{wave}}, \mathsf{I}_{\mathsf{wave}})$ be a trapdoor function used in Wave and $H \in \mathbb{F}_q^{(n-k)\times n}$ be a parity-check matrix for an (n,k)-code over $\mathbb{F}_q$. $\mathcal{X}_{n,t} = \{x \in \mathbb{F}_q^n : \mathsf{hw}(x) = t\}$ denotes a set of vectors $x \in \mathbb{F}_q^n$ whose Hamming weight is exactly t, where t is chosen such that $\mathsf{F}_{\mathsf{wave}} \colon \mathcal{X}_{n,t} \to \mathbb{F}_q^{n-k}$ is a surjection. $\mathsf{Gen}_{\mathsf{wave}}$ outputs a parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ for an (n,k)-code over $\mathbb{F}_q$ as $\mathsf{F}_{\mathsf{wave}}$ and parity-check matrices of generalized $(U, U+V)$-codes as $\mathsf{I}_{\mathsf{wave}}$. On input $x \in \mathcal{X}_{n,t}$, the function $\mathsf{F}_{\mathsf{wave}}$ computes a syndrome $y \coloneqq xH^T \in \mathbb{F}_q^{n-k}$. On input $y \in \mathbb{F}_q^{n-k}$, the trapdoor $\mathsf{I}_{\mathsf{wave}}$ outputs an element of $\mathcal{X}_{n,t}$. Since a description of $\mathsf{I}_{\mathsf{wave}}$ is out of the scope of this paper, we omit the description.

$\mathsf{T}_{\mathsf{wave}}$ satisfies the conditions of ATPSF [17, Definition 2] and we can take a statistical bound on the distinguishing advantage of honestly generated signatures and simulated ones.

C.3 Original/Modified UOV Signature [39, 53]

Let $\mathsf{T}_{\mathsf{uov}} = (\mathsf{Gen}_{\mathsf{uov}}, \mathsf{F}_{\mathsf{uov}}, \mathsf{I}_{\mathsf{uov}})$ (resp., $\mathsf{T}_{\mathsf{muov}} = (\mathsf{Gen}_{\mathsf{muov}}, \mathsf{F}_{\mathsf{muov}}, \mathsf{I}_{\mathsf{muov}})$) be a trapdoor function used in the original (resp., modified) UOV signature. Note that $\mathsf{Gen}_{\mathsf{uov}} = \mathsf{Gen}_{\mathsf{muov}}$ and $\mathsf{F}_{\mathsf{uov}} = \mathsf{F}_{\mathsf{muov}}$. $\mathsf{Gen}_{\mathsf{uov}}$ generates an invertible affine map $\mathsf{S}\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a multivariate quadratic map $\mathsf{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$ defined as $\mathsf{P} = (p_1, p_2, \ldots, p_o)$, where

$$p_k(z^v, z^o) = \sum_{i \in [v+o]} \sum_{j \in [v]} \alpha_{i,j}^k z_i z_j,$$

and outputs $\mathsf{P} \circ \mathsf{S}$ as $\mathsf{F}_{\mathsf{uov}}$ and (P, S) as $\mathsf{I}_{\mathsf{uov}}$. Variables in P are called vinegar variables $z^v = (z_1, z_2, \ldots, z_v) \in \mathbb{F}_q^v$ and oil variables $z^o = (z_{v+1}, z_{v+2}, \ldots, z_{v+o}) \in \mathbb{F}_q^o$, where $n = v + o$. On input $y \in \mathbb{F}_q^o$, $\mathsf{I}_{\mathsf{uov}}$ chooses $z^v \leftarrow_\$ \mathbb{F}_q^v$ and outputs $x = \mathsf{S}^{-1}(z^v \| z^o)$ by solving a linear equation system $\mathsf{P}(z^v, \cdot) = y$. There is possibly no solution. In the original UOV signature, $\mathsf{I}_{\mathsf{uov}}$ retries z^v until $\{z^o : \mathsf{P}(z^v, z^o) = y\} \neq \emptyset$ holds or $\mathsf{P}(z^v, \cdot)$ has full rank [11] (see Fig. 13). Since $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ is not uniformly distributed, we must assume the computational indistinguishability of $x \leftarrow \mathsf{I}_{\mathsf{uov}}(y)$ for $y \leftarrow_\$ \mathbb{F}_q^o$ and $x \leftarrow_\$ \mathbb{F}_q^n$ for the provable security.

The modified UOV signature adopts the probabilistic hash-and-sign with retry and does not retake the vinegar variables z^v. The signing procedure of the modified UOV signature (see Fig. 14) is different from the other signature schemes adopting the probabilistic hash-and-sign with retry. $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ using $\mathsf{I}_{\mathsf{muov}}^1$ and $\mathsf{I}_{\mathsf{muov}}^2$ generates a signature as follows: $\mathsf{I}_{\mathsf{muov}}^1$ chooses vinegar variables z^v uniformly at random. Fixing z^v, P becomes a set of linear functions on oil variables z^o. $\mathsf{I}_{\mathsf{muov}}^2$ finds a preimage of $\mathsf{P} \circ \mathsf{S}$ by solving a linear equation system and taking the inverse of S. If there is no solution, $\mathsf{I}_{\mathsf{muov}}^2$ outputs $\perp$ and $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}]$ retries r and executes $\mathsf{I}_{\mathsf{muov}}^2$ again without retrying z^v. Sakumoto et al. showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{muov}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. For completeness, we give the proof sketch.

In the beginning, z^v is uniformly chosen, that is, z^v follows $\mathsf{U}(\mathbb{F}_q^v)$. By fixing z^v, $\mathsf{P}(z^v, \cdot)$ becomes a set of linear functions containing $o \times o$ matrix whose rank is determined by choice of z^v if solutions exist. When the rank is i, $\mathsf{P}(z^v, \cdot)$ becomes a q^{o-i}-to-1 mapping for each element in the range $\mathbb{F}_q^o$. There are only q^i possible outputs of H satisfying $\{z^o : \mathsf{P}(z^v, z^o) = \mathsf{H}(r, m)\} \neq \emptyset$. When H is a random function, one of the q^i outputs is uniformly chosen after some retries.

Once the output is fixed, one of q^{o-i} solutions is uniformly chosen. In this way, z^o follows $\mathsf{U}(\mathbb{F}_q^o)$ and thus $x = \mathsf{S}^{-1}(z^v \| z^o)$ follows $\mathsf{U}(\mathbb{F}_q^n)$.

In Proposition 4, we cannot take q'_{sign} as in the other schemes since the probability that $\mathsf{I}_{\mathsf{muov}}(z^v, y)$ outputs $\perp$ varies depending on z^v. We set $q'_{\mathsf{sign}} = q_{\mathsf{retry}} q_{\mathsf{sign}}$, where q_{retry} is a bound on the number of queries to H in each signing query. Let X_i be a random variable for the number of queries to H in i-th queries and $X = \sum_{i=1}^{q_{\mathsf{sign}}} X_i$. We have

$$\Pr[X_i > q_{\mathsf{retry}}] = \sum_{j=1}^{o} p_j (1 - q^{j-o})^{q_{\mathsf{retry}}},$$

where p_j is a probability that $\mathsf{P}(z^v, \cdot)$ has rank j for $z^v \leftarrow_{\$} \mathbb{F}_q^v$. It is known that a random $o \times o$ matrix over $\mathbb{F}_q$ has rank $o - a$ for $a \in \{0, 1, \dots, o\}$ with a probability [7]:

$$\frac{1}{q^{a^2}} \cdot \frac{\prod_{k=1}^{o}(1 - q^{-k}) \prod_{k=a+1}^{o}(1 - q^{-k})}{\prod_{k=1}^{o-a}(1 - q^{-k}) \prod_{k=1}^{a}(1 - q^{-k})}. \tag{13}$$

When we assume that $\mathsf{P}(z^v, \cdot)$ becomes a random $o \times o$ matrix for any z^v, p_j follows Eq. (13). Since $X > q'_{\mathsf{sign}}$ implies $\exists i, X_i > q_{\mathsf{retry}}$, $\Pr[X > q'_{\mathsf{sign}}] \leq q_{\mathsf{sign}} \Pr[X_i > q_{\mathsf{retry}}]$ holds. To determine an appropriate value for $q'_{\mathsf{sign}} = q_{\mathsf{retry}} q_{\mathsf{sign}}$ in the security bound, we need to take q_{retry} such that $q_{\mathsf{sign}} \Pr[X_i > q_{\mathsf{retry}}]$ is negligible for the security parameter.

C.4 Modified HFE Signature [53]

The modified HFE signature adopts the probabilistic hash-and-sign with retry. Let $\mathsf{T}_{\mathsf{mhfe}} = (\mathsf{Gen}_{\mathsf{mhfe}}, \mathsf{F}_{\mathsf{mhfe}}, \mathsf{I}_{\mathsf{mhfe}})$ be a trapdoor function used in the modified HFE signature and $\phi \colon K \to \mathbb{F}_q^n$ be a standard linear isomorphism $\phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \dots, a_{n-1})$, where $K = \mathbb{F}_q[x]/g(x)$ for an irreducible polynomial $g(x)$ of degree n. $\mathsf{Gen}_{\mathsf{mhfe}}$ generates invertible affine maps $(\mathsf{S}, \mathsf{S}')$ over $\mathbb{F}_q^n$ and a central map $\mathsf{P} \colon K \to K$ defined as

$$\mathsf{P}(X) = \sum_{\substack{(i,j) \in [n] \times [n] \\ \text{s.t. } q^{i-1} + q^{j-1} < d}} \alpha_{i,j} X^{q^{i-1} + q^{j-1}} + \sum_{\substack{i \in [n] \\ \text{s.t. } q^{i-1} < d}} \beta_i X^{q^{i-1}},$$

where $\alpha_{i,j}, \beta_i \in K$, and outputs $\mathsf{S}' \circ \phi \circ \mathsf{P} \circ \phi^{-1} \circ \mathsf{S}$ as $\mathsf{F}_{\mathsf{mhfe}}$ and $(\mathsf{P}, \mathsf{S}, \mathsf{S}')$ as $\mathsf{I}_{\mathsf{mhfe}}$. On input $y \in \mathbb{F}_q^{n-m}$, $\mathsf{I}_{\mathsf{mhfe}}$ computes a preimage $x \in \mathbb{F}_q^n$ as in Fig. 15.

As in the modified UOV signature, the authors of [53] showed that preimages generated by $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. We give the proof sketch.

When H is a random function, each $z \in \mathbb{F}_q^n$ is chosen with probability $\frac{1}{q^n}$. With probability $\frac{|\{z' : \mathsf{P}(z') = z\}|}{N}$, $\mathsf{I}_{\mathsf{mhfe}}$ chooses z' out of $|\{z' : \mathsf{P}(z') = z\}|$ elements,

```
$\mathsf{I}_{\mathsf{mhfe}}(y)$
$y' \leftarrow_\$ \mathbb{F}_q^m$
$z := \phi^{-1}(\mathsf{S}'^{-1}(y \| y'))$
$i \leftarrow_\$ [N]$
if $1 \leq i \leq \left|\{z' : \mathsf{P}(z') = z\}\right|$ then
    return $\perp$
$z' \leftarrow_\$ \{z' : \mathsf{P}(z') = z\}$
$x := \mathsf{S}^{-1}(\phi(z'))$
return $x$
```

Fig. 15: Trapdoor of the modified HFE signature

where N is set as d in general. Therefore, for any $x \in \mathbb{F}_q^n$, $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}].\mathsf{Sign}$ outputs x with probability

$$\frac{1}{q^n} \cdot \frac{|\{z' : \mathsf{P}(z') = z\}|}{N} \cdot \frac{1}{|\{z' : \mathsf{P}(z') = z\}|} = \frac{1}{q^n N}.$$

Hence, preimages output by $\mathsf{HaS}[\mathsf{T}_{\mathsf{mhfe}}, \mathsf{H}].\mathsf{Sign}$ are uniformly distributed over $\mathbb{F}_q^n$. Also, $\mathsf{I}_{\mathsf{mhfe}}$ does not output $\perp$ with probability $\sum_{x \in \mathbb{F}_q^n} \frac{1}{q^n N} = \frac{1}{N}$, and we can take $q'_{\mathsf{sign}} = cNq_{\mathsf{sign}}$ for some constant $c > 1$ in Proposition 5.

C.5 MAYO [10]

MAYO adopts the probabilistic hash-and-sign. Let $\mathsf{T}_{\mathsf{mayo}} = (\mathsf{Gen}_{\mathsf{mayo}}, \mathsf{F}_{\mathsf{mayo}}, \mathsf{I}_{\mathsf{mayo}})$ be a trapdoor function used in MAYO. $\mathsf{Gen}_{\mathsf{mayo}}$ generates a multivariate quadratic map $\mathsf{P} \colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ with a subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension o called *oil space* such that $\mathsf{P}(x) = 0$ for any $x \in \mathcal{O}$, and outputs P as $\mathsf{F}_{\mathsf{mayo}}$ and a basis of $\mathcal{O}$ as $\mathsf{I}_{\mathsf{mayo}}$[13]. Let $\mathsf{P}(x) = (p_1(x), \ldots, p_m(x))$, where $p_i(x) \colon \mathbb{F}_q^n \to \mathbb{F}_q$ is a multivariate quadratic polynomial. The polar form of $p(x)$ is defined as

$$p'(x, y) := p(x + y) - p(x) - p(y),$$

which is bilinear. We define the polar form of multivariate quadratic map $\mathsf{P}(x)$ to be $\mathsf{P}'(x, y) = (p'_1(x, y), \ldots, p'_m(x, y))$.

Let $\mathcal{I} = \{(i, j) \in [k] \times [k] : i < j\}$ and $\{E_{ij}\}_{(i,j) \in \mathcal{I}}$ be a set of invertible matrices such that $E = \{E_{i,j}\}$ is nonsingular. We set $\{E_{ij}\}_{(i,j) \in \mathcal{I}}$ as a system parameter. On input $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^{kn}$, $\mathsf{F}_{\mathsf{mayo}}$ computes $y = \mathsf{P}^*(x) = \sum_{i \in [k]} E_{i,i} \mathsf{P}(x_i) + \sum_{(i,j) \in \mathcal{I}} E_{i,j} \mathsf{P}'(x_i, x_j)$. In MAYO, $\mathsf{P}^* \colon \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ is conjectured to be non-invertible. Therefore, the INV game of $\mathsf{T}_{\mathsf{mayo}}$ is defined as: given $(\mathsf{P}, \{E_{ij}\}_{(i,j) \in \mathcal{I}}, y)$, find $x^* = (x_1^*, \ldots, x_k^*)$ satisfying $\sum_{i \in [k]} E_{i,i} \mathsf{P}(x_i^*) + \sum_{(i,j) \in \mathcal{I}} E_{i,j} \mathsf{P}'(x_i^*, x_j^*)$ [10, Definition 2]. On input $y \in \mathbb{F}_q^m$, $\mathsf{I}_{\mathsf{mayo}}$ computes x as in Fig. 16. Let x, x^o and x^v be vectors over $\mathbb{F}_q^{kn}$. $\mathsf{I}_{\mathsf{mayo}}$ finds a preimage $x = x^v + x^o$ of y for P^*. In the beginning, x^v is uniformly chosen from $(\mathbb{F}_q^{n-o} \times \{0^o\})^k \subset \mathbb{F}_q^{kn}$,

[13] The notation of UOV in MAYO follows [9] which is a generalization of the traditional description of Appendix C.3.

```
$\mathsf{I}_{\mathsf{mayo}}(y)$
$\mathsf{P}^*(x_1, \ldots, x_k) := \sum_{i \in [k]} E_{i,i}\mathsf{P}(x_i) + \sum_{(i,j) \in \mathcal{I}} E_{i,j}\mathsf{P}'(x_i, x_j)$
repeat
    $x^v \leftarrow_\$ (\mathbb{F}_q^{n-o} \times 0^o)^k$
until $\mathsf{P}^*(x^v + x^o)$ has full rank
$x^o \leftarrow \{x^o : \mathsf{P}^*(x^v + x^o) = y\}$
$x = x^v + x^o$
return $x$
```

Fig. 16: Trapdoor of MAYO

where 0^o denotes a vector of o 0s. Fixing x^v, $\mathsf{P}^*(x^v + x^o) = y$ becomes a linear system of equations for $x^o \in \mathcal{O}^k$. If $\mathsf{P}^*(x^v + x^o)$ has full rank, $\mathsf{I}_{\mathsf{mayo}}$ outputs $x^v + x^o$ by solving $\mathsf{P}^*(x^v + x^o) = y$. Otherwise, $\mathsf{I}_{\mathsf{mayo}}$ retries x^v. The probability that $\mathsf{P}^*(x^v + x^o)$ does not have full rank is bounded by $\tau = \frac{q^{k-n+o} + q^{m-ko}}{q-1}$ [10, Lemma 1].

A preimage $x \leftarrow \mathsf{I}_{\mathsf{mayo}}(y)$ is uniform over $\mathbb{F}_q^{kn}$ if $\mathsf{I}_{\mathsf{mayo}}$ does not retry x^v in the signature generation [10, Lemma 2]. Since this property is necessary for applying Theorem 1, we show the proof sketch.

First, x^v is uniformly chosen from $(\mathbb{F}_q^{n-o} \times \{0^o\})^k$ if $\mathsf{I}_{\mathsf{mayo}}$ does not retry x^v. Next, x^o is uniformly chosen from $\mathcal{O}^k$ since $\mathsf{P}^*(x^v + x^o)$ has full rank. Hence, the output $x = x^v + x^o$ follows $\mathsf{U}(\mathbb{F}_q^{kn})$ since $(\mathbb{F}_q^{n-o} \times \{0^o\}) + \mathcal{O} = \mathbb{F}_q^n$ holds.

C.6 GPV Framework [30]

Signature schemes based on the GPV framework adopt the deterministic or probabilistic hash-and-sign. Let $\mathsf{T}_{\mathsf{gpv}} = (\mathsf{Gen}_{\mathsf{gpv}}, \mathsf{F}_{\mathsf{gpv}}, \mathsf{I}_{\mathsf{gpv}})$ be a trapdoor function used in the GPV framework. $\mathsf{Gen}_{\mathsf{gpv}}$ outputs a full-rank matrix $A \in \mathbb{Z}_q^{n \times m}$ generating a q-ary lattice Λ as $\mathsf{F}_{\mathsf{gpv}}$ and a matrix B generating $\Lambda_q^\perp$ that is orthogonal to Λ modulo q as $\mathsf{I}_{\mathsf{gpv}}$. The function $\mathsf{F}_{\mathsf{gpv}}$ computes $y = xA^T$ for a short vector $x \in \{x \in \mathbb{Z}^m : \|x\| \leq s\sqrt{m}\}$, where s is a Gaussian parameter. The trapdoor $\mathsf{I}_{\mathsf{gpv}}$ outputs a short vector x for $y \in \mathbb{F}_q^n$ using B. $\mathsf{T}_{\mathsf{gpv}}$ is a collision-resistant PSF (see Definition 6) whose security is based on the hardness of the short integer solution (SIS) problem [30, Theorem 4.9].

D Proof of Lemma 6

First, we extend Theorem 1 to prove the following lemma:

Lemma 8 (M-INV $\Rightarrow$ M-EUF-CMA). *For any quantum* M-EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ *of* $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}}, \mathsf{H}, \mathsf{E}]$ *with* q_{key} *keys and issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U} \times \mathcal{R} \times \mathcal{M}}$, *there exist an* M-INV $\mathcal{B}_{\mathsf{inv}^{\mathsf{m}}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *with* q_{key} *instances and an* M-PS *adversary* $\mathcal{D}_{\mathsf{ps}^{\mathsf{m}}}$ *of* $\mathsf{T}_{\mathsf{wpsf}}$ *with* q_{key} *instances and issuing* q_{sign} *sampling*

```
GAME: M-EUF-NMA
for $j \in [q_{\mathsf{key}}]$ do
    $(vk_j, sk_j) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$
$(j^*, m^*, \sigma^*) \leftarrow \mathcal{A}_{\mathsf{nma^m}}(\{vk_j\}_{j \in [q_{\mathsf{key}}]})$
return $\mathsf{Sig.Verify}(vk_{j^*}, m^*, \sigma^*)$
```

Fig. 17: M-EUF-NMA (Multi-key EUF-NMA) game

queries such that

$$\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma^m}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\text{M-INV}}_{\mathsf{T_{wpsf}}}(\mathcal{B}_{\mathsf{inv^m}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T_{wpsf}}}(\mathcal{D}_{\mathsf{ps^m}}) + \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}} + \frac{q^2_{\mathsf{key}}}{|\mathcal{U}|}, \quad (14)$$

where q'_{sign} is a bound on the total number of queries to H in all the signing queries and the running times of $\mathcal{B}_{\mathsf{inv^m}}$ and $\mathcal{D}_{\mathsf{ps^m}}$ are about that of $\mathcal{A}_{\mathsf{cma^m}}$.

Proof. We prove two reductions; M-EUF-NMA ⇒ M-EUF-CMA and M-INV ⇒ M-EUF-CMA, where M-EUF-NMA stands for *multi-key* EUF-NMA. We define an advantage function of the M-EUF-NMA game given in Fig. 17 as $\mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{Sig}}(\mathcal{A}_{\mathsf{nma^m}}) = \Pr[\mathsf{M\text{-}EUF\text{-}NMA}^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1]$. Without loss of generality, we assume that adversaries make random oracle queries while fixing key ID u to be one of the q_{key} verification keys.

M-EUF-NMA ⇒ M-EUF-CMA*:*

GAME G_0 (M-EUF-CMA game): This is the original M-EUF-CMA game and $\Pr[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1] = \mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma^m}})$ holds.

GAME G_1 (adaptive reprogramming and puncturing of H): In the same manner as G_4 of Theorem 1, the challenger chooses $r \leftarrow_{\$} \mathcal{R}$ for $q'_{\mathsf{sign}} - q_{\mathsf{sign}}$ times and keeps them in a sequence $\mathcal{S}$, punctures H by $\mathcal{S}' = \{u \in \mathcal{U}, r \in \mathcal{S}, m \in \mathcal{M}\}$, and outputs 0 if FIND $= \top$. Also, the signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(\mathsf{E}(\mathsf{F}_j), r_i, m_i) \mapsto y_i}$ after repeating $r_i \leftarrow \mathcal{R}$ and $y_i \leftarrow_{\$} \mathcal{Y}$ until $\mathsf{I}_j(y_i)$ does not output $\perp$. In Theorem 1, we can derive the bounds on the advantage gaps of $\mathsf{G}_0/\mathsf{G}_1$, $\mathsf{G}_1/\mathsf{G}_2$, and $\mathsf{G}_3/\mathsf{G}_4$ by analyzing the number of queries to H, the number of times H is reprogrammed, and the number of punctured points of H. Since these numbers are the same in both the single-key and multi-key settings, we have

$$\left|\Pr[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1] - \Pr[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1]\right| \leq \frac{3}{2}q'_{\mathsf{sign}}\sqrt{\frac{q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}}+2)\sqrt{\frac{q'_{\mathsf{sign}}-q_{\mathsf{sign}}}{|\mathcal{R}|}}.$$

GAME G_2 (simulating the signing oracle by $\mathsf{SampDom}$): The signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(\mathsf{E}(\mathsf{F}_j), r_i, m_i) \mapsto \mathsf{F}_j(x_i)}$ for $r_i \leftarrow \mathcal{R}$ and $x_i \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$, and outputs (r_i, x_i). Since the M-PS adversary can simulate $\mathsf{G}_1/\mathsf{G}_2$, we have $\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T_{wpsf}}}(\mathcal{D}_{\mathsf{ps^m}})$.

Since the M-EUF-NMA adversary $\mathcal{A}_{\mathsf{nma^m}}$ can simulate G_2 by $\mathsf{SampDom}$, $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma^m}}} \Rightarrow 1\right] \leq \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma^m}})$ holds.

As above, we have

$$\mathrm{Adv}^{\text{M-EUF-CMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma^m}}) \leq \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma^m}}) + \mathrm{Adv}^{\text{M-PS}}_{\mathsf{T_{wpsf}}}(\mathcal{D}_{\mathsf{ps^m}}) + \frac{3}{2} q'_{\mathsf{sign}} \sqrt{\frac{q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1}{|\mathcal{R}|}} + 2(q_{\mathsf{qro}} + 2)\sqrt{\frac{q'_{\mathsf{sign}} - q_{\mathsf{sign}}}{|\mathcal{R}|}}. \quad (15)$$

M-INV ⇒ M-EUF-NMA*:*

Game G_3 (M-EUF-NMA game): This is the original M-EUF-NMA game and $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS^{ph}}[\mathsf{T_{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{nma^m}})$ holds.

Game G_4 (abort with the collision on key IDs): When a collision on the key IDs is detected, G_4 aborts and outputs 0. From the collision probability of uniformly chosen key IDs, $\left|\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]\right| \leq \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$.

We use Lemma 2 to show a reduction from the M-INV assumption of $\mathsf{T_{wpsf}}$. The M-INV adversary $\mathcal{B}_{\mathsf{inv^m}}$ given $\{(\mathsf{F}_j, y_j)\}_{j \in [q_{\mathsf{key}}]}$ runs a two-stage algorithm S that runs $\mathcal{A}_{\mathsf{nma^m}}$ playing G_4. In the second stage, the input θ of S_2 is chosen from $\{y_j\}_{j \in [q_{\mathsf{key}}]}$. A two-stage algorithm S composed of S_1 and S_2 operates as follows:

1. Choose $(i, b) \leftarrow_{\$} ([q_{\mathsf{qro}}] \times \{0,1\}) \cup \{(q_{\mathsf{qro}} + 1, 0)\}$.
2. Run $\mathcal{A}_{\mathsf{nma^m}}$ with H until i-th query.
3. Measure i-th query and output (u, r, m) as the output of S_1.
4. Given a random θ, reprogram $\mathsf{H}' = \mathsf{H}^{(u,r,m) \mapsto \theta}$.
5. If $i = q_{\mathsf{qro}} + 1$, then go to Step 8.
6. Answer i-th query with H (if $b = 0$) or H' (if $b = 1$).
7. Run $\mathcal{A}_{\mathsf{nma^m}}$ with H' until the end.
8. Output $\mathcal{A}_{\mathsf{nma^m}}$'s output (j^*, m^*, r^*, x^*) as the output of S_2.

Since there is no collision on key IDs, $\mathcal{B}_{\mathsf{inv^m}}$ can understand the target key of the observed random oracle query. If $u = \mathsf{E}(\mathsf{F}_j)$, $\mathcal{B}_{\mathsf{inv^m}}$ sets $\theta = y_j$, reprograms H as $\mathsf{H}' := \mathsf{H}^{(u,r,m) \mapsto y_j}$, and uses $\mathsf{F}_j(x) \overset{?}{=} \mathsf{H}(u, r, m)$ as the predicate. From Lemma 2, we have the following for any $\hat{j} \in [q_{\mathsf{key}}]$:

$$\Pr\left[j = \hat{j} \wedge \mathsf{F}_j(x) = y_j : (\mathsf{E}(\mathsf{F}_j), r, m) \leftarrow \mathsf{S}_1^{\mathcal{A}}(), (j, m, r, x) \leftarrow \mathsf{S}_2^{\mathcal{A}}(y_j)\right]$$
$$\geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[j = \hat{j} \wedge \mathsf{F}_j(x) = \mathsf{H}\left(\mathsf{E}(\mathsf{F}_j), r, m\right) : (j, m, r, x) \leftarrow \mathcal{A}_{\mathsf{nma^m}}^{|\mathsf{H}\rangle}\left(\{\mathsf{F}_j\}_{j \in [q_{\mathsf{key}}]}\right)\right]$$

By summing over all $\hat{j} \in [q_{\mathsf{key}}]$, we have $\mathrm{Adv}^{\text{M-INV}}_{\mathsf{T_{wpsf}}}(\mathcal{B}_{\mathsf{inv^m}}) \geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma^m}}} \Rightarrow 1\right]$. We obtain Eq. (14) by combining the two reductions. □

Then, we extend the proof of M-INV $\Rightarrow$ M-EUF-NMA in Lemma 8 by introducing a new game G_5. In G_5, the verification keys $\{\mathsf{F}_j\}_{j \in [q_{\mathsf{key}}]}$ are replaced with $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}$, where $\mathsf{F}' \colon \mathcal{X}' \to \mathcal{Y}$ is generated by Gen' of the trapdoor function T'. The ST adversary $\mathcal{D}_{\mathsf{st}}$ can simulate $\mathsf{G}_4/\mathsf{G}_5$ by setting the verification keys based on the outcomes of querying NewKey_b. When $\mathcal{D}_{\mathsf{st}}$ plays ST_0, we simulate G_4; otherwise, we simulate G_5. This leads to $\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{nma}^\mathsf{m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma}^\mathsf{m}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}})$.

To apply Lemma 2, we assume that the INV adversary $\mathcal{B}_{\mathsf{inv}}$ against T' employs a two-stage algorithm S within G_5. As with Lemma 8, $\mathcal{B}_{\mathsf{inv}}$ possesses knowledge of the target key for the observed query. When the observed value targets the j-th verification key, $\mathcal{B}_{\mathsf{inv}}$ sets $\mathsf{L}_j(y)$ as the input to S_2. Because L_j is bijective, $\mathsf{L}_j(y)$ for $y \leftarrow_\$ \mathcal{Y}$ follows a uniform distribution. When $\mathcal{A}_{\mathsf{nma}^\mathsf{m}}$ submits x for F_j, $\mathcal{B}_{\mathsf{inv}}$ returns $\mathsf{R}_j(x)$. If $\mathsf{L}_j(\mathsf{F}(\mathsf{R}_j(x))) = \mathsf{L}_j(y)$ holds, since L_j is a bijection, we conclude that $\mathsf{F}(\mathsf{R}_j(x)) = y$. In summary, $\mathcal{B}_{\mathsf{inv}}$ can win the INV game by submitting $\mathsf{R}_j(x)$, yielding $\mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{inv}}) \geq \frac{1}{(2q_{\mathsf{qro}}+1)^2} \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{nma}^\mathsf{m}}} \Rightarrow 1\right]$. Therefore, we have:

$$\mathrm{Adv}^{\text{M-EUF-NMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{wpsf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^\mathsf{m}}) \leq (2q_{\mathsf{qro}}+1)^2 \mathrm{Adv}^{\mathrm{INV}}_{\mathsf{T}'}(\mathcal{B}_{\mathsf{inv}}) + \mathrm{Adv}^{\mathrm{ST}}_{\mathsf{T}_{\mathsf{wpsf}},\mathsf{T}'}(\mathcal{D}_{\mathsf{st}}) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}. \tag{16}$$

By combining Eq. (15) and Eq. (16), we arrive at Eq. (11). □

E Proof of Lemma 7

First, we show a reduction of M-CR $\Rightarrow$ M-sEUF-CMA extending the single-key version of [14, Theorem 2].

Lemma 9 (M-CR $\Rightarrow$ M-EUF-CMA). *For any quantum* M-sEUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}^\mathsf{m}}$ *of* $\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]$ *with* q_{key} *keys and issuing at most* q_{sign} *classical queries to the signing oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_\$ \mathcal{Y}^{\mathcal{U}\times\mathcal{R}\times\mathcal{M}}$*, there exist an* M-CR $\mathcal{B}_{\mathsf{cr}^\mathsf{m}}$ *of* $\mathsf{T}_{\mathsf{psf}}$ *with* q_{key} *instances such that*

$$\mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}[\mathsf{T}_{\mathsf{psf}},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) \leq \frac{1}{1-2^{-\omega(\log(\lambda))}} \mathrm{Adv}^{\text{M-CR}}_{\mathsf{T}_{\mathsf{psf}}}(\mathcal{B}_{\mathsf{cr}^\mathsf{m}}) + \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}, \tag{17}$$

where the running times of $\mathcal{B}_{\mathsf{cr}^\mathsf{m}}$ *and* $\mathcal{D}_{\mathsf{st}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}^\mathsf{m}}$*.*

Proof. We define a sequence of games as follows:

Game G_0 (M-sEUF-CMA game): This is the original M-sEUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}^\mathsf{m}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{M-sEUF-CMA}}_{\mathsf{HaS}^{\mathsf{ph}}[\mathsf{T}_{\mathsf{psf}},\mathsf{H},\mathsf{E}]}(\mathcal{A}_{\mathsf{cma}^\mathsf{m}})$ holds.

Game G_1 (abort with collision on key IDs): When a collision of the key IDs is detected, G_1 aborts and outputs 0. We have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{nma}^\mathsf{m}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma}^\mathsf{m}}} \Rightarrow 1\right]\right| \leq \frac{q_{\mathsf{key}}^2}{|\mathcal{U}|}$.

Game G_2 (replacing H with H'): This game replaces H with H' satisfying

$$\mathsf{H}'\left(\mathsf{E}\left(\mathsf{F}_j\right), r, m\right) = \mathsf{F}_j\left(\mathsf{DetSampDom}\left(\mathsf{F}_j, \widetilde{\mathsf{H}}\left(\mathsf{E}\left(\mathsf{F}_j\right), r, m\right)\right)\right),$$

where $\mathsf{DetSampDom}$ is a deterministic function of $\mathsf{SampDom}$ and $\widetilde{\mathsf{H}}\colon \mathcal{U} \times \mathcal{R} \times \mathcal{M} \to \mathcal{W}$ is another random function to output randomness for $\mathsf{DetSampDom}$. Since $\mathsf{E}(\mathsf{F}_j) \neq \mathsf{E}(\mathsf{F}_{j'})$ for any $j, j' \in [q_{\mathsf{key}}]$, we can uniquely identify F_j based on $\mathsf{E}(\mathsf{F}_j)$. Therefore, it is feasible to program H'. From **Condition 1** of PSF, $\mathsf{F}_j(x)$ is uniform for $x \leftarrow \mathsf{SampDom}(\mathsf{F}_j)$. Therefore, H and H' follow the same distribution and $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{nma}^{\mathsf{m}}}} \Rightarrow 1\right]$ holds.

The M-CR adversary $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ can simulate G_2. From **Conditions 2** and **3**, the M-CR adversary $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ can simulate the signing oracle. When responding to the i-th signing query m_i for the j-th verification key F_j, $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ returns (r_i, x_i), where $r_i \leftarrow_{\$} \mathcal{R}$ and $x_i := \mathsf{DetSampDom}\left(\mathsf{F}_j, \widetilde{\mathsf{H}}\left(\mathsf{E}\left(\mathsf{F}_j\right), r_i, m_i\right)\right)$. If the M-sEUF-CMA adversary $\mathcal{A}_{\mathsf{cma}^{\mathsf{m}}}$ wins the game by submitting (j^*, m^*, r^*, x^*), $\mathsf{F}_{j^*}(x^*) = \mathsf{F}_{j^*}(x')$ holds, where $x' = \mathsf{DetSampDom}(\mathsf{F}_{j^*}, \widetilde{\mathsf{H}}(\mathsf{E}(\mathsf{F}_{j^*}), r^*, m^*)))$. From **Condition 4**, $x^* \neq x'$ holds with probability $1 - 2^{-\omega(\log(\lambda))}$, and we thus have Eq. (17). □

Then, we show a reduction of CR ⇒ M-CR. We define a sequence of games as follows:

Game G_0 (M-CR game): This is the original M-CR game and $\Pr\left[\mathsf{G}_0^{\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}} \Rightarrow 1\right] = \mathrm{Adv}_{\mathsf{T}_{\mathsf{psf}}}^{\text{M-CR}}(\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}})$ holds.

Game G_1 (replacing verification keys): We replace F_j with $\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j$. Since the ST adversary can simulate $\mathsf{G}_0/\mathsf{G}_1$, we have $\left|\Pr\left[\mathsf{G}_0^{\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}_{\mathsf{T}_{\mathsf{psf}}, \mathsf{T}'}^{\text{ST}}(\mathcal{D}_{\mathsf{st}})$.

The CR adversary $\mathcal{B}_{\mathsf{cr}}$ simulates G_1 as follows: Given F', $\mathcal{B}_{\mathsf{cr}}$ gives $\{\mathsf{L}_j \circ \mathsf{F}' \circ \mathsf{R}_j\}_{j \in [q_{\mathsf{key}}]}$ to $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$. When $\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}$ submits (j^*, x_1^*, x_2^*), $\mathcal{B}_{\mathsf{cr}}$ outputs $(\mathsf{R}_{j^*}(x_1^*), \mathsf{R}_{j^*}(x_2^*))$. Suppose that $\mathsf{L}_{j^*}(\mathsf{F}(\mathsf{R}_{j^*}(x_1^*))) = \mathsf{L}_{j^*}(\mathsf{F}(\mathsf{R}_{j^*}(x_2^*)))$ holds. Since L_{j^*} and R_{j^*} are injective, $\mathsf{F}(\mathsf{R}_{j^*}(x_1^*)) = \mathsf{F}(\mathsf{R}_{j^*}(x_2^*))$ holds and $x_1^* \neq x_2^*$ implies $\mathsf{R}_{j^*}(x_1^*) \neq \mathsf{R}_{j^*}(x_2^*)$. Therefore, $\mathcal{B}_{\mathsf{cr}}$ can win the CR game and can perfectly simulate G_4. Therefore, we have

$$\mathrm{Adv}_{\mathsf{T}_{\mathsf{psf}}}^{\text{M-CR}}(\mathcal{B}_{\mathsf{cr}^{\mathsf{m}}}) \leq \mathrm{Adv}_{\mathsf{T}'}^{\text{CR}}(\mathcal{B}_{\mathsf{cr}}) + \mathrm{Adv}_{\mathsf{T}_{\mathsf{psf}}, \mathsf{T}'}^{\text{ST}}(\mathcal{D}_{\mathsf{st}}). \tag{18}$$

Combining Eq. (18) with Eq. (17), we obtain the security bound of Lemma 7. □

F Applications of Generic Method in Multi-key Setting

In this section, we explore the applications of the generic method presented in Lemma 7 for lattice-based cryptography and Lemma 6 for code-based and MQ-based cryptography. Rather than focusing on specific schemes such as FALCON [52], our paper applies the generic method to frameworks of the schemes, such as the GPV framework [30]. We leave the applicability to the specific schemes for future works.

Lattice-based Cryptography: We apply the generic method to the GPV framework (see Appendix C.6) [30]. For Lemma 7, we design simulation of verification keys by $\{L_j A R_j\}_{j \in [q_{\mathsf{key}}]}$ where L_j is an $n \times n$ invertible matrix over $\mathbb{F}_q$ and R_j is an $m \times m$ signed permutation matrix. In the GPV framework, the domain of the trapdoor function is a set of short vectors $\{x \in \mathbb{Z}^m : |x| \leq s\sqrt{m}\}$, where s is a Gaussian parameter. Accordingly, we define R_j as an orthogonal matrix to ensure $\|x\| = \|x R_j^T\|$, and any integer orthogonal matrices are signed permutation matrices, characterized by non-zero entries ± 1. Then, the ST advantage is bounded by an advantage of the following problem.

Definition 12 (Multi-instance Signed Permutation Equivalence). *Given matrices $\{G_j\}_{j \in [q_{\mathsf{key}}]}$ ($G_j \in \mathbb{F}_q^{n \times m}$), do there exist a matrix $G \in \mathbb{F}_q^{n \times m}$, $n \times n$ invertible matrices $\{L_j\}_{j \in [q_{\mathsf{key}}]}$ over $\mathbb{F}_q$, and $m \times m$ signed permutation matrices $\{R_j\}_{j \in [q_{\mathsf{key}}]}$ over $\mathbb{F}_q$ such that $G_j = L_j G R_j$?*

This problem is a variant of the well-studied problem called *code equivalence* in code-based cryptography [51]. The code equivalence is defined as: Given a pair of matrices (G, G'), do there exist an invertible matrix L and an isometric matrix R such that $G' = LGR$? There are variations of this problem in terms of R. When R is a permutation matrix (resp., generalized permutation matrix), this problem is called *permutation equivalence* (resp., *linear equivalence*)[55].

In lattice-based cryptography, there is a closely related problem called *lattice isomorphism*, that is, given a pair of lattice bases (B, B'), do there exist a unimodular matrix L and an orthogonal matrix R such that $B' = LBR$? The conditions on L and R are required to keep the geometry of lattices; however, it is not necessary for our purpose.

Any variants of the code equivalence listed above are in the complexity class coAM and not conjectured to be NP-hard [51]. Also, there are some algorithms for the permutation equivalence and linear equivalence. In the general case, Leon's algorithm solves the problems by enumerating all the codewords with Hamming weight w for some w [40], and Beullens [8] recently improved this algorithm. The complexity of this approach grows exponentially with w, and we cannot solve the problems with low w [4]. There is a special case where we can easily solve the permutation equivalence with the Support Splitting Algorithm (SSA) proposed by Sendrier [54]. The SSA runs in $O(m^3 + m^2 q^h \ln(m))$, where h is a dimension of the hull space of a code, that is, the intersection between the code and its dual code [4]. Therefore, the SSA can efficiently solve the permutation equivalence if the dimension of the hull space is low. Note that the SSA does not apply to the case with an empty hull.

Code-based Cryptography: We apply the generic method to a trapdoor function using a parity-check matrix $H \in \mathbb{F}_q^{n \times m}$ as in the modified CFS signature and Wave (see Appendices C.1 and C.2). For Lemma 6, we simulate verification keys by $\{L_j H R_j\}_{j \in [q_{\mathsf{key}}]}$, where L_j is an $m \times m$ invertible matrix over $\mathbb{F}_q$ and R_j is an $n \times n$ generalized permutation matrix over $\mathbb{F}_q$. In the modified CFS signature and Wave, the domain of the trapdoor function is a set of vectors whose Hamming weight is either a constant or bounded by a constant. To ensure this, we define

R_j as a generalized permutation matrix that preserves the Hamming weights of vectors. Then, the ST advantage is bounded by an advantage of the following problem.

Definition 13 (Multi-instance Linear Equivalence). *Given matrices $\{G_j\}_{j\in[q_{\mathsf{key}}]}$ ($G_j \in \mathbb{F}_q^{n\times m}$), do there exist a matrix $G \in \mathbb{F}_q^{n\times m}$, $n \times n$ invertible matrices $\{L_j\}_{j\in[q_{\mathsf{key}}]}$ over $\mathbb{F}_q$, and $m \times m$ generalized permutation matrices $\{R_j\}_{j\in[q_{\mathsf{key}}]}$ over $\mathbb{F}_q$ such that $G_j = L_j G R_j$?*

As mentioned in the previous paragraph, some algorithms exist for the (single-instance) linear equivalence.

Multivariate-quadratic-based Cryptography: We assume a trapdoor function of the original/modified UOV signature or the modified HFE signature. Let $\mathsf{F}\colon \mathbb{F}_q^{n'} \to \mathbb{F}_q^m$ and $\mathsf{F}_j\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a multivariate quadratic map ($n' \geq n$). For Lemma 6, we simulate verification keys by $\{\mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$, where L_j is an invertible affine map over $\mathbb{F}_q$ and R_j is an affine map over $\mathbb{F}_q$. Then, the ST advantage is bounded by an advantage of the following game.

Definition 14 (Multi-instance Decision Morphism of Polynomials). *Given multivariate quadratic maps $\{\mathsf{F}_j\}_{j\in[q_{\mathsf{key}}]}$, do there exist a multivariate quadratic map F and affine maps $\{\mathsf{L}_j\}_{j\in[q_{\mathsf{key}}]}$ and $\{\mathsf{R}_j\}_{j\in[q_{\mathsf{key}}]}$ over $\mathbb{F}_q$ such that $\mathsf{F}_j = \mathsf{L}_j \circ \mathsf{F} \circ \mathsf{R}_j$?*

The (single-instance) decision morphism of polynomials, that is, given a pair of multivariate quadratic maps $(\mathsf{F}, \mathsf{F}')$, do there exist affine maps L and R such that $\mathsf{F}' = \mathsf{L} \circ \mathsf{F} \circ \mathsf{R}$?, is proven NP-complete [50]. If L and R are invertible affine maps, this problem is called *decision isomorphism of polynomials* that is in the complexity class coAM and not conjectured to be NP-hard [50]. For signature schemes with some structures in their verification key, only invertible R may preserve the structures, e.g., only block-anti-circulant matrices can maintain a structure of BAC-UOV [57]; therefore, we need to use invertible R as in the decision isomorphism of polynomials for such signature schemes.

A search version of the isomorphism of polynomials has been well-studied. Bouillaguet, Fouque, and Véber [15] studied and surveyed the algorithms for the isomorphism of polynomials. Their algorithms run in $O(q^n) \cdot \mathsf{poly}(n, q)$, $O(q^{2n/3}) \cdot \mathsf{poly}(n, q)$, or $O(q^{n/2}) \cdot \mathsf{poly}(n, q)$ assuming that $n = m$. The Gröbner-based algorithm proposed by Faugère and Perret [27] can efficiently solve random instances of an *inhomogeneous* version of the problem. We also note that if L and R are very structured, then the problems become easier (see, e.g., [36]).

G Security Proof of Fiat-Shamir with Aborts

We define a 3-round public-coin identification scheme with aborts.

Definition 15 (3-round Public-coin Identification Scheme with Aborts). *A 3-round public-coin identification scheme with aborts, denoted as* ID*, consists of four algorithms:*

```
GAME: A-HVZK_b
  $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
  $b^* \leftarrow \mathcal{D}_{\mathsf{zk}}^{\mathsf{Sample}_b}(pk)$
  return $b^*$

Sample_0()
  repeat
      $(w_i, st_i) \leftarrow \mathsf{P}_1(sk)$
      $c_i \leftarrow_\$ \mathcal{C}$
      $z_i \leftarrow \mathsf{P}_2(sk, w_i, c_i, st_i)$
  until $z_i \neq \bot$
  return $(w_i, c_i, z_i)$

Sample_1()
  $(w_i, c_i, z_i) \leftarrow \mathsf{Sim}(pk)$
  return $(w_i, c_i, z_i)$
```

Fig. 18: Accepting HVZK Game

```
FSwA[ID, H].KeyGen(1^λ)
  $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
  return $(pk, sk)$

FSwA[ID, H].Sign(sk, m)
  repeat
      $(w, st) \leftarrow \mathsf{P}_1(sk)$
      $c := \mathsf{H}(w, m)$
      $z \leftarrow \mathsf{P}_2(sk, w, c, st)$
  until $z \neq \bot$
  return $(w, z)$

FSwA[ID, H].V(pk, m, (w, z))
  $c := \mathsf{H}(w, m)$
  return $\mathsf{V}(pk, w, c, z)$
```

Fig. 19: Algorithms of the Fiat-Shamir with aborts

$\mathsf{Gen}(1^\lambda)$: *This algorithm takes the security parameter* 1^λ *as input and outputs a public key* pk *and a secret key* sk*.*

$\mathsf{P}_1(sk)$: *This algorithm takes a secret key* sk *as input and outputs a commitment* $w \in \mathcal{W}$ *and a state* st*.*

$\mathsf{P}_2(sk, w, c, st)$: *This algorithm takes a secret key* sk*, a commitment* $w \in \mathcal{W}$*, a randomly chosen challenge* $c \leftarrow_\$ \mathcal{C}$*, and a state* st *as input and outputs a response* $z \in \mathcal{Z}$ *or outputs* $\bot$*.*

$\mathsf{V}(pk, w, c, z)$: *This algorithm takes a public key* pk*, a commitment* $w \in \mathcal{W}$*, a challenge* $c \in \mathcal{C}$*, and a response* $z \in \mathcal{Z}$ *(a transcript) as inputs and outputs* $\top$ *(acceptance) or* $\bot$ *(rejection).*

Let Sim denote a simulator for ID, which takes a public key pk as its input and yields a transcript in the form of (w, c, z) as its output. To establish the indistinguishability between a transcript generated honestly and one generated through simulation, we introduce an accepting HVZK game.

Definition 16 (Accepting HVZK (A-HVZK) Game [3, Definition 1]). *Let* ID *be a 3-round public-coin identification scheme with aborts. Using a game defined in Fig. 18, we define an advantage function of an adversary playing the* A-HVZK *game against* ID *as* $\mathrm{Adv}_{\mathsf{ID}}^{\text{A-HVZK}}(\mathcal{D}_{\mathsf{zk}}) = \left|\Pr\left[\text{A-HVZK}_0^{\mathcal{D}_{\mathsf{zk}}} \Rightarrow 1\right] - \Pr\left[\text{A-HVZK}_1^{\mathcal{D}_{\mathsf{zk}}} \Rightarrow 1\right]\right|$*. We say* ID *is accepting HVZK if its advantage is negligible for any efficient adversary.*

We can construct a signature scheme, denoted as $\mathsf{FSwA}[\mathsf{ID}, \mathsf{H}]$, from ID as depicted in Fig. 19. The security reduction for this scheme can be provided using the same techniques as presented in Theorem 1.

Theorem 2 (EUF-NMA ⇒ EUF-CMA). *For any quantum* EUF-CMA *adversary* $\mathcal{A}_{\mathsf{cma}}$ *of* $\mathsf{FSwA}[\mathsf{ID}, \mathsf{H}]$ *issuing at most* q_{sign} *classical queries to the signing* *oracle and* q_{qro} *(quantum) random oracle queries to* $\mathsf{H} \leftarrow_{\$} \mathcal{C}^{\mathcal{W}\times\mathcal{M}}$*, there exist an* EUF-NMA *adversary* $\mathcal{A}_{\mathsf{nma}}$ *of* $\mathsf{FSwA}[\mathsf{ID},\mathsf{H}]$ *issuing* q_{qro} *(quantum) random oracle queries to* H *and an* A-HVZK *adversary* $\mathcal{D}_{\mathsf{zk}}$ *of* ID *issuing* q_{sign} *sampling queries such that*

$$\begin{aligned}\mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{FSwA}[\mathsf{ID},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}}) &\le \mathrm{Adv}^{\text{EUF-NMA}}_{\mathsf{FSwA}[\mathsf{ID},\mathsf{H}]}(\mathcal{A}_{\mathsf{nma}}) + \mathrm{Adv}^{\text{A-HVZK}}_{\mathsf{ID}}(\mathcal{D}_{\mathsf{zk}}) \\ &+\frac{3}{2}q'_{\mathsf{sign}}\sqrt{(q'_{\mathsf{sign}}+q_{\mathsf{qro}}+1)\,\epsilon} + 4(q_{\mathsf{qro}}+2)\sqrt{(q'_{\mathsf{sign}}-q_{\mathsf{sign}})\,\epsilon},\end{aligned} \tag{19}$$

where q'_{sign} *is a bound on the total number of queries to* H *in all the signing queries,* $\max_{\hat{w}\in\mathcal{W}} \Pr[w = \hat{w} : (w, st) \leftarrow \mathsf{P}_1(sk)] \le \epsilon$ *holds except with negligible probability, and the running times of* $\mathcal{A}_{\mathsf{nma}}$ *and* $\mathcal{D}_{\mathsf{zk}}$ *are about that of* $\mathcal{A}_{\mathsf{cma}}$*.*

Proof. As in Theorem 1, we can set $q'_{\mathsf{sign}} = \frac{c}{\rho} q_{\mathsf{sign}}$ for some constant $c > 1$, where $\rho = \Pr[z \ne \bot : (w, st) \leftarrow \mathsf{P}_1(sk), c \leftarrow_{\$} \mathcal{C}, z \leftarrow \mathsf{P}_2(sk, w, c, st)]$. To show Eq. (19), we use a sequence of games defined in Fig. 20.

Game G_0 (EUF-CMA game): This is the original EUF-CMA game and $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \mathrm{Adv}^{\text{EUF-CMA}}_{\mathsf{FSwA}[\mathsf{ID},\mathsf{H}]}(\mathcal{A}_{\mathsf{cma}})$ holds.

Game G_1 (adaptive reprogramming of H): The signing oracle $\mathsf{Sign}^{\mathsf{H}}$ adaptively reprograms H. This reprogramming occurs as $\mathsf{H} := \mathsf{H}^{(w_i,m_i)\mapsto c_i}$, where $(w_i, st_i) \leftarrow \mathsf{P}_1(sk)$ and $c_i \leftarrow \mathcal{C}$, and this process repeats until $\mathsf{P}_2(sk, w_i, c_i, st_i)$ no longer outputs $\bot$. The AR adversary $\mathcal{D}_{\mathsf{ar}}$ can simulate the games G_0 and G_1. When $\mathcal{D}_{\mathsf{ar}}$ playes AR_0, it simulates G_0; othereise, it simulates G_1. According to Lemma 1, the difference between $\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ and $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$ can be bounded as follows:

$$\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \le \mathrm{Adv}^{\mathrm{AR}}_{\mathsf{H}}(\mathcal{D}_{\mathsf{ar}}) \le \frac{3}{2} q'_{\mathsf{sign}}\sqrt{(q'_{\mathsf{sign}} + q_{\mathsf{qro}} + 1)\epsilon}.$$

Game G_2 (pre-generating transcripts): At the start, the challenger pre-generates q_{sign} accepting transcripts for ID along with non-accepting ones. An accepting transcript is stored as (w_i, c_i, z_i), and non-accepting transcripts (excluding responses) are stored in $\mathcal{S}_i$. During the i-th signing query, the signing oracle reprograms H as $\mathsf{H}^{(w,m_i)\mapsto c}$ for $(w, c) \in \mathcal{S}_i$ as well as for (w_i, c_i). This pre-generation of transcripts is feasible since they are chosen independently of queried messages m_i from $\mathcal{A}_{\mathsf{cma}}$ in G_1, ensuring that $\Pr\left[\mathsf{G}_1^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$.

Game G_3 (puncturing H): Let $\mathcal{S} = \{w : (w, *) \in \bigcup_i \mathcal{S}_i\}$ and $\mathcal{S}' = \{(w, m) : w \in \mathcal{S}, m \in \mathcal{M}\}$. We define a punctured oracle $\mathsf{H}\backslash\mathcal{S}'$ and an event FIND as in Definition 10. In G_3, $\mathcal{A}_{\mathsf{cma}}$ makes queries to $\mathsf{H}\backslash\mathcal{S}'$, and G_3 outputs 0 if FIND $= \top$. Assume that $\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\rangle}(\mathsf{F})\right]$. Since G_3 differs from G_2 in two aspects: the use of $\mathsf{H}\backslash\mathcal{S}'$ and the output of 0 when FIND $= \top$, $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[1 \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign},|\mathsf{H}\backslash\mathcal{S}'\rangle}(\mathsf{F}) \wedge \text{FIND} = \bot\right]$ and

```
GAME: $\mathsf{G}_0$-$\mathsf{G}_1$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{C}^{\mathcal{W} \times \mathcal{M}}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$(m^*, w^*, z^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(pk)$
if $m^* \in \mathcal{Q}$ then
    return $0$
$c^* := \mathsf{H}(w^*, m^*)$
return $\mathsf{V}(pk, w^*, c^*, z^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_0$
repeat
    $(w_i, st_i) \leftarrow_\$ \mathsf{P}_1(sk)$
    $c_i := \mathsf{H}(w_i, m_i)$
    $z_i \leftarrow \mathsf{P}_2(sk, w_i, c_i, st_i)$
until $z_i \neq \bot$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(w_i, z_i)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_1$
repeat
    $(w_i, st_i) \leftarrow_\$ \mathsf{P}_1(sk)$
    $c_i \leftarrow_\$ \mathcal{C}$
    $z_i \leftarrow \mathsf{P}_2(sk, w_i, c_i, st_i)$
    $\mathsf{H} := \mathsf{H}^{(w_i, m_i) \mapsto c_i}$
until $z_i \neq \bot$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(w_i, z_i)$
```

```
GAME: $\mathsf{G}_2$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{C}^{\mathcal{W} \times \mathcal{M}}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
for $i \in [q_{\mathsf{sign}}]$ do
    $\mathcal{S}_i := \emptyset$
    repeat
        $(w, st) \leftarrow \mathsf{P}_1(sk)$
        $c \leftarrow \mathcal{C}$
        $z \leftarrow \mathsf{P}_2(sk, w, c, st)$
        if $z = \bot$ then
            $\mathcal{S}_i := \mathcal{S}_i \cup \{(w, c)\}$
        else
            $(w_i, c_i, z_i) := (w, c, z)$
    until $z \neq \bot$
$(m^*, w^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(pk)$
if $m^* \in \mathcal{Q}$ then
    return $0$
$c^* := \mathsf{H}(w^*, m^*)$
return $\mathsf{V}(pk, w^*, c^*, z^*)$
```

```
GAME: $\mathsf{G}_3$-$\mathsf{G}_4$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{C}^{\mathcal{W} \times \mathcal{M}}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
$\mathcal{S} = \emptyset$
for $i \in [q_{\mathsf{sign}}]$ do
    $\mathcal{S}_i := \emptyset$
    repeat
        $(w, st) \leftarrow \mathsf{P}_1(sk)$
        $c \leftarrow \mathcal{C}$
        $z \leftarrow \mathsf{P}_2(sk, w, c, st)$
        if $z = \bot$ then
            $\mathcal{S}_i := \mathcal{S}_i \cup \{(w, c)\}$
            $\mathcal{S} := \mathcal{S} \cup \{w\}$
        else
            $(w_i, c_i, z_i) := (w, c, z)$
    until $z \neq \bot$
$\mathcal{S}' = \{(w, m) : w \in \mathcal{S}, m \in \mathcal{M}\}$
$\mathrm{FIND} = \bot$
$(m^*, w^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H} \setminus \mathcal{S}'\rangle}(pk)$
if $m^* \in \mathcal{Q} \vee \mathrm{FIND} = \top$ then
    return $0$
$c^* := \mathsf{H}(w^*, m^*)$
return $\mathsf{V}(pk, w^*, c^*, z^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_2$-$\mathsf{G}_3$
for $(w, c) \in \mathcal{S}_i$ do
    $\mathsf{H} := \mathsf{H}^{(w, m_i) \mapsto c}$
$\mathsf{H} := \mathsf{H}^{(w_i, m_i) \mapsto c_i}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(w_i, z_i)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_4$
$\mathsf{H} := \mathsf{H}^{(w_i, m_i) \mapsto c_i}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(w_i, z_i)$
```

```
GAME: $\mathsf{G}_5$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{C}^{\mathcal{W} \times \mathcal{M}}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
for $i \in [q_{\mathsf{sign}}]$ do
    repeat
        $(w, st) \leftarrow \mathsf{P}_1(sk)$
        $c \leftarrow \mathcal{C}$
        $z \leftarrow \mathsf{P}_2(sk, w, c, st)$
    until $z \neq \bot$
    $(w_i, c_i, z_i) := (w, c, z)$
$(m^*, w^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(pk)$
if $m^* \in \mathcal{Q}$ then
    return $0$
$c^* := \mathsf{H}(w^*, m^*)$
return $\mathsf{V}(pk, w^*, c^*, z^*)$
```

```
GAME: $\mathsf{G}_6$
$\mathcal{Q} := \emptyset$
$\mathsf{H} \leftarrow_\$ \mathcal{C}^{\mathcal{W} \times \mathcal{M}}$
$(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
for $i \in [q_{\mathsf{sign}}]$ do
    $(w_i, c_i, z_i) \leftarrow \mathsf{Sim}(pk)$
$(m^*, w^*, x^*) \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\rangle}(pk)$
if $m^* \in \mathcal{Q}$ then
    return $0$
$c^* := \mathsf{H}(w^*, m^*)$
return $\mathsf{V}(pk, w^*, c^*, z^*)$
```

```
$\mathsf{Sign}^{\mathsf{H}}(m_i)$ for $\mathsf{G}_5$-$\mathsf{G}_6$
$\mathsf{H} := \mathsf{H}^{(w_i, m_i) \mapsto c_i}$
$\mathcal{Q} := \mathcal{Q} \cup \{m_i\}$
return $(w_i, z_i)$
```

Fig. 20: Games for EUF-NMA ⇒ EUF-CMA for Fiat-Shamir with aborts. The modifications from the previous game are highlighted in red text.

$\Pr\left[\text{FIND} = \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \; = \; \Pr\left[\text{FIND} = \top : b \leftarrow \mathcal{A}_{\mathsf{cma}}^{\mathsf{Sign}, |\mathsf{H}\backslash\mathcal{S}'\rangle}(\mathsf{F})\right]$ hold. Applying Lemma 4,

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \sqrt{(q_{\mathsf{qro}} + 2) \Pr\left[\text{FIND} = \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]}. \tag{20}$$

We will show a bound on Eq. (20) after defining G_4.

Game G_4 (reprogramming only for successful trials): The signing oracle reprograms $\mathsf{H} := \mathsf{H}^{(w_i, m_i) \mapsto c_i}$ only for accepting transcripts. It's important to note that $\mathcal{A}_{\mathsf{cma}}$ makes queries to the punctured oracle $\mathsf{H}\backslash\mathcal{S}'$. If FIND $= \bot$, then $\mathcal{A}_{\mathsf{cma}}$ cannot obtain $\mathsf{H}(w, m)$ for $(w, m) \in \mathcal{S}'$. Therefore, if FIND $= \bot$, $\mathcal{A}_{\mathsf{cma}}$ cannot distinguish whether H is reprogrammed at $(w, m) \in \mathcal{S}'$ in G_3 or not in G_4. From Lemma 3, we have

$$\Pr\left[\text{FIND} = \bot : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\text{FIND} = \bot : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]. \tag{21}$$

Especially, if G_3 or G_4 outputs 1, then FIND must be $\bot$. Therefore, we conclude that $\Pr\left[\mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]$. Also, $\Pr\left[\text{FIND} {=} \top : \mathsf{G}_3^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] = \Pr\left[\text{FIND} {=} \top : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right]$ holds from Eq. (21).

We show a bound on Eq. (20). Let G'_4 be a modified G_4 played by $\mathcal{B}_{\mathsf{cma}}$. $\mathcal{B}_{\mathsf{cma}}$ outputs (w', m') and wins the game if $(w', m') \in \mathcal{S}'$. Choosing $j \leftarrow_{\$} [q_{\mathsf{qro}} + 1]$, $\mathcal{B}_{\mathsf{cma}}$ runs $\mathcal{A}_{\mathsf{cma}}$ playing G_4. Just before $\mathcal{A}_{\mathsf{cma}}$ makes j-th query to H, $\mathcal{B}_{\mathsf{cma}}$ measures a query input register of $\mathcal{A}_{\mathsf{cma}}$ and outputs the measurement outcome as (w', m'). The oracles of G'_4 reveal no information on $\mathcal{S}$ and $\mathcal{S}'$. If we assume that $\max_{\hat{w} \in \mathcal{W}} \Pr[w = \hat{w} : (w, st) \leftarrow \mathsf{P}_1(sk)] \leq \epsilon$ holds, then $\Pr\left[\mathsf{G}'^{\mathcal{B}_{\mathsf{cma}}}_4 \Rightarrow 1\right] \leq \Pr[w' \in \mathcal{S}] \leq (q'_{\mathsf{sign}} - q_{\mathsf{sign}})\epsilon$ holds. From Lemma 5, we have

$$\Pr\left[\text{FIND} = \top : \mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow b\right] \leq 4(q_{\mathsf{qro}} + 1)(q'_{\mathsf{sign}} - q_{\mathsf{sign}})\epsilon.$$

Hence, an upper bound on Eq. (20) is $2(q_{\mathsf{qro}} + 2)\sqrt{(q'_{\mathsf{sign}} - q_{\mathsf{sign}})\epsilon}$.

Game G_5 (Canceling the punctuation on H): The challenger no longer punctures H, and we remove the unused $\mathcal{S}_i$, $\mathcal{S}$, and $\mathcal{S}'$ from the game. By applying Lemma 4, we obtain the same bound as Eq. (20):

$$\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq 2(q_{\mathsf{qro}} + 2)\sqrt{(q'_{\mathsf{sign}} - q_{\mathsf{sign}})\epsilon}.$$

Game G_6 (simulating the signing oracle by Sim): The challenger generates $(w_i, c_i, z_i) \leftarrow \mathsf{Sim}(pk)$ for $i \in [q_{\mathsf{sign}}]$. The A-HVZK adversary $\mathcal{D}_{\mathsf{zk}}$ can simulate G_5 and G_6. If $\mathcal{D}_{\mathsf{zk}}$ plays $\mathsf{A\text{-}HVZK}_0$, the procedures of the original and simulated G_5 are identical. If $\mathcal{D}_{\mathsf{zk}}$ plays $\mathsf{A\text{-}HVZK}_1$, he obviously simulates G_6. Therefore, we have:

$$\left|\Pr\left[\mathsf{G}_5^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_6^{\mathcal{A}_{\mathsf{cma}}} \Rightarrow 1\right]\right| \leq \mathrm{Adv}_{\mathsf{ID}}^{\text{A-HVZK}}(\mathcal{D}_{\mathsf{ps}}).$$

Since G_6 can be simulated without using sk, the EUF-NMA adversary $\mathcal{A}_{\mathsf{nma}}$ can simulate G_6. Summing up, we have Eq. (19) for EUF-NMA ⇒ EUF-CMA. □

Notice that Theorem 2 does not yield a worse bound than [3, Theorem 2], except for a factor of 2 in the last term of Eq. (19).